E-Mail Security

امنیت پست الکترونیکی



- ✓ مفاهیم پایه‌ای پست الکترونیکی
- ✓ مخاطرات پست الکترونیکی
- ✓ مکانیزم‌های ایمن‌سازی پست الکترونیکی
- ✓ پروتکل‌های پست الکترونیکی
- ✓ ارائه روشی نوین برای ارزیابی مخاطرات پست الکترونیکی
- ✓ ایمن‌سازی مخاطرات پست الکترونیکی بر اساس نوع سازمان

مولف: مهندس سید حسین رجاء
کارشناس ارشد فناوری اطلاعات
موسسه تحقیقاتی داده‌سنجی پیشرفته

امنیت پست الکترونیکی

سید حسین رجاء



درباره این کتاب: از ویژگی‌های این کتاب، ارائه روشی نوین برای ارزیابی مخاطرات پست الکترونیکی و نیز، ایمن‌سازی مخاطرات پست الکترونیکی، بر اساس نوع سازمان می‌باشد. مقالات متعددی بر اساس این کتاب، در همایش‌ها و مجلات از سوی نویسنده ارائه شده و به چاپ رسیده است. مخاطبین اصلی کتاب، کارشناسان پست الکترونیکی، کارشناسان امنیت، مدیران شبکه، دانشجویان نرم‌افزار، متخصصین لینوکس و علاقه‌مندان به حوزه پست الکترونیکی می‌باشند.

درباره نویسنده: سید حسین رجاء کارشناس ارشد فناوری اطلاعات (IT) موسسه تحقیقاتی داده‌سنجی پیشرفته می‌باشد. وی ۱۴ سال سابقه فعالیت در زمینه‌های شبکه، امنیت شبکه و برنامه‌نویسی را دارد. از جمله مدارک علمی ایشان می‌توان به RHCSS ، CCSP، CCIE Routing and Switching و LPI 3 اشاره کرد. وی نصب، راه‌اندازی و مدیریت سرورهای Qmail، Sendmail، Postfix، Exim و Exchange Server در زمینه پست الکترونیکی را تجربه کرده است.

www.PendarePars.com

9786006529004

امنیت پست الکترونیکی

سید حسین رجاء

انتشارات پندار پارس

سرشناسه : رجاء، سیدحسین، ۱۳۶۲ -
عنوان و نام پدیدآور : امنیت پست الکترونیکی/ حسین رجاء.
مشخصات نشر : تهران : پندار پارس: مانلی، ۱۳۹۰.
مشخصات ظاهری : xi، ۱۶۰ ص.: مصور، نمودار.
شابک : ۴۵۰۰۰ ریال: ۹۷۸-۶۰۰-۶۵۲۹-۰۰-۴
وضعیت فهرست نویسی : فیپا
موضوع : پست الکترونیکی -- پیش‌بینی‌های ایمنی
موضوع : پست الکترونیکی
رده بندی کنگره : TK۵۱۰۵/۷۳ /۳ر۸الف ۱۳۹۰
رده بندی دیویی : ۶۹۲/۰۰۴
شماره کتابشناسی ملی : ۲۵۹۶۴۲۷

انتشارات پندارپارس
دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوچه رشتچی، شماره ١٤، واحد ١٦ **www.pendarepars.com**
تلفن: ٦٦٥٧٢٣٣٥ - تلفکس: ٦٦٩٢٦٥٧٨همراه: ٠٩١٢٢٤٥٢٣٤٨ **info@pendarepars.com**

نام کتاب : امنیت پست الکترونیکی
ناشر : انتشارات پندار پارس ناشر همکار: مانلی
تالیف : سید حسین رجاء
چاپ نخست : زمستان ۹۰
شمارگان : ۱۰۰۰ نسخه
طرح جلد : محمد اسماعیلی هدی
لیتوگرافی، چاپ، صحافی : ترام‌سنج، فرشیوه، خیام
قیمت : ٤٥٠٠ تومان شابک : ٩٧٨-٦٠٠-٦٥٢٩-٠٠-٤

بسم الله الرحمن الرحیم

تقدیم به:

سید و سالار شهیدان، حضرت امام حسین(ع)

و

ساحت مقدس مولایمان حضرت مهدی(عج) که حضرت امام موسی کاظم (ع) در توصیف فرزند عزیزشان فرموده‌اند:

او طرد شده تنهای غریب است ...

به‌نام خداوند جان و خرد

پیش‌گفتار

فن‌آوری پست الکترونیکی، با توجه به استفاده روز افزون از آن در عصر اطلاعات، به یکی از ملزومات زندگی بشر، برای مکاتبات و مراسلات بین افراد، تبدیل شده است. با توجه به این مسئله، نکته قابل اهمیت در مورد پست الکترونیکی این است که سرور و سرویس پست الکترونیکی و پیام‌ها و مکاتبات رد و بدل شده بین افراد، دارای امنیت قابل قبولی باشد تا افراد با اطمینان خاطر از این فن‌آوری، استفاده کنند.

ابتدا به بررسی نحوه عملکرد سیستم پست الکترونیکی و معرفی پروتکل‌های آن می‌پردازیم. با بررسی صورت گرفته مشخص شد که برای ارزیابی مخاطرات سیستم پست الکترونیکی، روش خاصی ارائه نشده است.

با بررسی روش‌های ارزیابی سایر سیستم‌ها و نقاط ضعف و قوت آنها، از روش آقای کانوری که روشی برای ارزیابی در حیطه امنیت شبکه می‌باشد، برای ارزیابی مخاطرات پست الکترونیکی استفاده می‌کنیم. با ارائه جداول خاص و استفاده از فرمول کانوری، به بررسی مخاطرات می‌پردازیم که معیار کار ما برای ارزیابی مخاطرات می‌باشد. پس از آن، به معرفی و بحث بر روی مخاطرات موجود در سرور و سرویس پست الکترونیکی می‌پردازیم.

سپس به مکانیزم‌های امن کردن مخاطرات سرور و سرویس پست الکترونیکی می‌پردازیم. میزان کاهش مخاطره را با به‌کارگیری مکانیزم‌ها و راهکارهای موجود، به صورت مطالعه موردی و به وسیله آزمایش‌هایی بدست می‌آوریم. در نهایت و در فصل نتیجه گیری، پست الکترونیکی را از لحاظ امنیت و نوع سازمان، دسته‌بندی کرده و مکانیزم‌های ایمن سازی آن را ارائه می‌دهیم.

مخاطبین اصلی کتاب، کارشناسان پست الکترونیکی، کارشناسان امنیت، مدیران شبکه، دانشجویان رشته نرم افزار، متخصصین لینوکس و تمامی افراد علاقه‌مند به حوزه پست الکترونیکی می‌باشند.

این کتاب با توجه به مطالعات علمی و تجربه فنی نگارنده در سرورهای پست الکترونیکی Qmail، Postfix، Sendmail، Exim و Exchange Server تألیف شده است. بدیهی است که مطالب این کتاب، خالی از اشکال نمی‌باشد و نظرات خوانندگان، ما را در بهبود سطح علمی و فنی کتاب، یاری خواهد کرد؛ لذا از خوانندگان محترم درخواست می‌شود هرگونه پیشنهاد و انتقادی در جهت بهبود و اصلاح محتویات کتاب را به آدرس الکترونیکی hosseinraja@dspri.com ارسال نمایند.

در نهایت بر خود لازم می‌دانم از موسسه تحقیقاتی داده‌سنجی پیشرفته، جناب مهندس مقدسی و جناب مهندس سید محمد رجاء، که اینجانب را در مراحل مختلف تألیف این کتاب یاری رسانده‌اند، کمال تشکر را داشته باشم.

سید حسین رجاء

پاییز ۱۳۹۰

فهرست

درباره مؤلف:

سید حسین رجاء کارشناس ارشد فناوری اطلاعات(IT) موسسه تحقیقاتی داده سنجی پیشرفته می‌باشد. وی حدوداً ۱۴ سال فعالیت در زمینه‌های مختلف IT، من جمله تدریس، برنامه نویسی، شبکه و امنیت شبکه را تجربه کرده است. ایشان علاوه بر موسسه تحقیقاتی داده سنجی پیشرفته، موسسه آموزش عالی خیام، شرکت مسیر فن‌آوری اطلاعات و شرکت فن‌آوران رجحان را در کارنامه کاری خود دارد. از جمله مدارک علمی ایشان می‌توان به CCIE Routing and Switching، CCSP، RHCSS و LPI 3(301 Open Ldap, 302 Mixed Environment, 303 Security, 305 Mail) اشاره کرد. وی در زمینه پست الکترونیکی، نصب، راه اندازی و مدیریت سرورهای Qmail، Sendmail، Postfix، Exim و Exchange Server را تجربه کرده است.

درباره این کتاب:

این کتاب به مسئله امنیت پست الکترونیکی می‌پردازد. ابتدا مفاهیم پست الکترونیکی و نحوه عملکرد پست الکترون‌یکی را خواهیم آموخت. در ادامه مخاطرات پست الکترونیکی، معرفی شده و به نحوه ایمن سازی آنها اشاره خواهیم کرد. از ویژگی‌های مهم این کتاب، ارائه روشی نوین برای ارزیابی مخاطرات پست الکترونیکی و همچنین، ایمن سازی مخاطرات پست الکترونیکی، بر اساس نوع سازمان می‌باشد. بر اساس این کتاب، مقالات متعددی در همایش‌ها و مجلات از سوی نویسنده ارائه شده و به چاپ رسیده است. مخاطبین اصلی کتاب، کارشناسان پست الکترونیکی، کارشناسان امنیت، مدیران شبکه، دانشجویان رشته نرم افزار، متخصصین لینوکس و تمامی افراد علاقه‌مند به حوزه پست الکترونیکی می‌باشند.

فصل اول

مقدمه

۱-۱ طرح مسئله

سال‌ها پیش، زمانی که پست الکترونیکی و رایانه‌ای وجود نداشت و سیستم مراسلات به صورت کاغذی و به شکل نامه بود، افراد از فاش شدن محتوای نامه خود هراس داشتند. مسائل مالی، از بین رفتن آبرو و حیثیت اشخاص، مسائل سیاسی، اجتماعی و فرهنگی از جمله دلایلی بودند که فکر امن کردن مراسلات و سیستم آن را به وجود آورد.

با پیشرفت علم و ورود به عرصه رایانه، بشر سیستم جدیدی برای مراسلاتش به وجود آورد. سیستم جدید که همان پست الکترونیکی بود، کار نامه کاغذی را با سرعتی بسیار بالاتر انجام می‌داد. همانند سیستم سنتی، مسئله‌ای که وجود داشت، بحث امنیت پیام‌های رد و بدل شده و همچنین امنیت سیستم ارسال مراسلات بود. البته اهمیت امنیت سیستم الکترونیکی، نسبت سیستم سابق، فزونی می‌یابد. در عصر اطلاعات، بسیاری از تراکنش‌ها چه مالی و چه غیرمالی، به صورت الکترونیکی انجام می‌شوند، تبادل داده‌ها از طریق اینترنت صورت می‌گیرد و سرقت و دستکاری و لو رفتن داده‌ها می‌تواند هزینه ای گزاف از حیث آبرویی، مالی، سیاسی، اقتصادی و فرهنگی داشته باشد.

در حوزه مراسلات الکترونیکی که پست الکترونیکی باشد، نیز این مسئله وجود دارد و بسی حائز اهمیت است[1].

در حوزه پست الکترونیکی، پروتکل‌ها و مکانیزم‌های مختلفی وجود دارد و درون این پروتکل‌ها و مکانیزم‌ها، انواع مخاطرات وجود دارد. مسئله مهم آن است که:

- مخاطرات را بشناسیم.
- چگونه این مخاطرات را ارزیابی کنیم.
- چگونه این مخاطرات را، از طریق مکانیزم‌های موجود، ایمن نماییم و مخاطره را کاهش دهیم.

- راهکار ایمن سازی پست الکترونیکی، بر اساس تقسیم‌بندی سـازمان‌هـا و ارزیـابی صـورت گرفته، ارائه دهیم.

افرادی مانند بولم[2] و اسمیت[12]، مخاطراتی را که برای پست الکترونیکی وجود دارند، به دو دسته کلی مخاطرات سرور پست الکترونیکی[1] و مخاطرات سرویس پست الکترونیکی تقسیم‌بندی کرده‌اند. در این کتاب، از این دسته بندی استفاده می‌کنیم. میزان مخاطرات را با فرمولی که ارائه داده ایم، بررسی کرده و میزان کاهش درصد مخاطره را، با راهکارها و مکانیزم‌های موجود، محاسبه می‌کنیم.

در مخاطراتی که برای سرور پست الکترونیکی وجود دارد می‌توان به موارد زیر اشاره کرد:

- فعال نبودن برخی ویژگی‌ها بر روی سرور پست الکترونیکـی، مـی‌توانـد باعـث بـه مخاطره افتادن سرور و سوء استفاده از آن گردد. این ویژگی‌ها را بررسی کـرده و نحوه فعال کردن آنها را بیان می‌کنیم.
- هنگامی که یک سرور پست الکترونیکی، تلاش می‌کنـد یـک نامـه مـرتبط بـه سـرور پست الکترونیکی دیگر را، به سـرور پسـت الکترونیکـی بفرسـتد و سـرور، پیـام را پذیرفته و به سرور پست الکترونیکی دیگر بفرستد، Open Relay اتفاق می‌افتد. اما سوء استفاده از این مسئله، موجب شده است که تمهیداتی در نظـر گرفتـه شـود تـا جلوی این مسئله گرفته شود[3]. در اینجا مکانیزم‌های رلـه کـردن گزینشـی، ارائـه می‌شود.
- با مواجه شدن با حجم انبوه پست‌های spam، ممکن است سـرور از کـار بیفتـد[4]. از ابتدای تولـد اینترنـت، متـدهای زیـادی بـرای جلـوگیری از spam، معرفـی شـده است[5]. سه متد کلی برای بلوک کردن spamها، تا به حال معرفی شده است.
- ویروس‌ها عنصر خطرناکی هستند. اثـر تخریبیشـان بسـیاری از مـدیران شـبکه را مجبور کرده است تا دنبال راهی برای متوقف کردن آنها بیابند[6].

در مخاطراتی که برای سرویس پست الکترونیکی وجود دارد، می‌توان به موارد زیر اشاره کرد:

- نفوذکنندگان و spammerها تکنیک‌های مختلفی اسـتفاده مـی‌کننـد تـا اطلاعـاتی در مورد سیستم پست الکترونیکی و کاربران آن بدست آورند، ولی تکنیک‌هایی وجـود دارد که کمک می‌کند تا بـا ایـن مشـکل، مبـارزه کنیـد. بـا غیـر فعـال کـردن برخـی

---

[1] Email Server

دستورات و همچنین نصب فایروال پست الکترونیکی، می‌توانید جلوی حملات و کاوشگری‌ها را بگیرید.

- متد رایج اجازه دادن به میزبان‌های راه دور، که بتوانند پیام‌ها را از طریق پست الکترونیکی سرور رله کنند، استفاده از یک متد تایید هویت می‌باشد. متد تایید هویت، به صورت منحصربه‌فرد می‌تواند پست الکترونیکی سرور راه دور را مشخص کند، به نحوی که پست الکترونیکی سرورتان بتواند مشخص کند اجازه دارد پیام‌ها را رله کند یا خیر. یکی از مشهورترین متدهای تایید هویت اتصالات شبکه، SASL[1] می‌باشد که به بررسی آن می‌پردازیم[8][7].
- بسیاری از بسته‌های MTA[2] برای دریافت پیام‌ها، از پروتکل‌های pop3[3] یا imap[4] بهره می‌گیرند[10][9]. مشکل این پروتکل‌ها این است که آنها اطلاعات را به صورت متن اسکی، بدون هیچ رمز نگاری ارسال می‌کنند. برای کمک کردن به این‌گونه مسائل، پروتکل SSL[5] به وجود آمد که به میزبان‌های شبکه اجازه می‌دهد تا داده‌ها را قبل از ارسالشان در طول شبکه، رمز کنند[11]. در این کتاب به شرح این پروتکل و پروتکل‌های مشابه آن می‌پردازیم.
- بسیاری از شرکت‌ها، نرم افزار کلاینتی پست الکترونیکی تحت وب، منتشر کرده‌اند که کاربر را قادر می‌سازد از طریق وب، پست الکترونیکی خود را بخواند. پیاده سازی‌های بسیار زیاد و محبوبی مانند Hotmail، Yahoo! و Gmail وجود دارد که کاربران می‌توانند از طریق پویش گر وب[6]، به سرور پست الکترونیکی متصل شوند[12]. Webmail به خودی خود امن نیست و باید راهکارهای ایمن سازی را برای آن پیاده سازی کنیم.

با ارائه جدول و فرمولی خاص، به سنجش و بررسی مخاطرات می‌پردازیم که در اخذ راهکارهای امنیتی کمک قابل توجهی می‌کند.

[1] Simple Authentication and Security Layer
[2] Mail Transfer Agent
[3] Post Office Protocol version 3
[4] Internet Message Access Protocol
[5] Secured Socket Layer
[6] Web Browser

۱-۲ اهداف

مضامین اصلی که در کتاب مورد بحث قرار خواهد گرفت، به شرح زیر است:

- بررسی نحوه عملکرد سیستم پست الکترونیکی.
- بررسی و معرفی پروتکل‌های پست الکترونیکی، همانند pop، imap، smtp[۱] و mime[۲]
- بررسی مخاطرات موجود برای سرور پست الکترونیکی.
- بررسی مخاطرات موجود برای سرویس پست الکترونیکی.
- ارائه جدول مخاطره و فرمول خاص، برای محاسبه مخاطرات.
- بررسی راهکارها و مکانیزم‌های تأمین امنیت سرور پست الکترونیکی.
- بررسی راهکارها و مکانیزم‌های تأمین امنیت سرویس پست الکترونیکی.
- بررسی میزان تأثیر راهکارها و مکانیزم‌ها و محاسبه میزان تقلیل مخاطره، به صورت موردی.
- ارائه دسته بندی پست‌های الکترونیکی، چگونگی ایمن سازی آنها و نتیجه گیری.

۱-۳ پرسش‌ها و فرضیات

مسئله‌ای که در قسمت طرح مسئله ارائه شد، مجدداً برای تاکید ذکر می‌کنیم:

در حوزه پست الکترونیکی، پروتکل‌ها و مکانیزم‌های مختلفی وجود دارد و درون این پروتکل‌ها و مکانیزم‌ها انواع مخاطرات وجود دارد. مسئله مهم آن است که:

- مخاطرات را بشناسیم.
- چگونه این مخاطرات را ارزیابی کنیم.
- چگونه این مخاطرات را، از طریق مکانیزم‌های موجود، ایمن نماییم و مخاطره را کاهش دهیم.

---

[1] Simple Mail Transfer Protocol
[2] Multipurpose Internet mail extensions

- راهکار ایمن سازی پست الکترونیکی، بر اساس تقسیم بندی سازمان‌ها و ارزیابی صورت گرفته، ارائه دهیم.

حال با توجه به مسئله موجود، پرسش‌ها و فرضیاتی پدید می‌آید که بایستی آنها را مطرح کنیم.

پرسش‌های موجود برای این تحقیق، عبارتند از:

- آیا مخاطرات موجود در پروتکل‌ها و مکانیزم‌های پست الکترونیکی را می‌توان شناخت؟
- آیا می‌توان این مخاطرات را ارزیابی کرد؟
- آیا روشی برای ارزیابی مخاطرات پست الکترونیکی وجود دارد؟
- آیا می‌توان از روش‌های ارزیابی موجود در دیگر سیستم‌ها، برای ارزیابی پست الکترونیکی استفاده نمود؟
- نقاط قوت و ضعف روش‌های ارزیابی در سیستم‌های دیگر چیست؟
- آیا پارامترهای موجود در ارزیابی مخاطرات سایر سیستم‌ها، با مکانیزم‌ها و پروتکل‌های سیستم پست الکترونیکی نیز رابطه دارند؟
- آیا می‌توان مخاطرات موجود در پست الکترونیکی را با روش‌های موجود، ایمن نمود؟
- آیا می‌توان میزان کاهش مخاطره را پس از ایمن سازی محاسبه کرد؟
- آیا می‌توان راهکاری جامع بر اساس تقسیم بندی سازمان‌ها و میزان مخاطره ارائه داد؟

فرضیه‌های موجود در این کتاب، عبارتند از:

- سیستم پست الکترونیکی که دارای مکانیزم‌ها و پروتکل‌های مختلفی می‌باشد. این مکانیزم‌ها و پروتکل‌ها، حاوی مخاطراتی می‌باشند و می‌توان این مخاطرات را شناسایی کرد.
- می‌توان مخاطرات موجود در سیستم‌های پست الکترونیکی را ارزیابی کرد.
- می‌توان از روش‌های ارزیابی مخاطراتی که در سایر سیستم‌ها وجود دارد، برای سیستم پست الکترونیکی نیز استفاده نمود.

- پارامترهـای موجـود در ارزیـابی مخـاطرات سـایر سیسـتمهـا، بـا مکـانیزمهـا و پروتکلهای سیستم پست الکترونیکی نیز رابطه دارند.
- میتوان مخاطرات موجود در پست الکترونیکی را با روشهای موجود ایمن نمود.
- میتوان میزان کاهش مخاطره را، پس از ایمن سازی محاسبه کرد.
- میتوان راهکاری جامع بر اساس تقسیم بندی سازمانهـا و میـزان مخـاطره، ارائـه داد.

۱-۴ تحقیقات مرتبط

در این کتاب، پس از بررسی مخاطرات سرور و سیستم پست الکترونیکی، با ارائه جدول و فرمولی خاص، مخاطرات را مورد ارزیابی قرار میدهیم. با بررسی صورت گرفته، در حوزه مخاطرات سیستمهای پست الکترونیکی و ارزیابی آن، روش خاصی ارائه نشده است اما در حوزه مخاطرات سیستمهای دیگر، تحقیقاتی صورت گرفته و روش هایی ارائه شده است.

استون برنر و همکارانش، در حوزه مخاطرات سیستمهای بر مبنای IT، فرمولی ارائه دادهاند که بسیاری از افراد در ارزیابی مخاطرات، از آن استفاده میکنند. این فرمول از دو پارامتر احتمال کلی[1] و تأثیر[2] استفاده میکند[13]. فرمول در قالب توصیه نامهای از سازمان NIST[3] ارائه شده است و افراد مختلف با تغییر نام پارامترها، فرمول را به همان شیوه ارائه شده، استفاده میکنند. برای مثال در حوزه امنیت نرم افزار و شبکه، مک گراو[4] فرمولی ارائه داده است که از دو پارامتر انتظار کاهش تنها[5] و نرخ رخداد در سال[6]، برای محاسبه مخاطره استفاده میکند[14]. این فرمول، در واقع همان پارامترهای تغییر نام یافتهای است که در فرمول استون برنر و همکارانش ارائه شده است. البته افرادی وجود دارند که از فرمولهای دیگر و پارامترهای اضافه تری استفاده کردهاند. برای مثال در حملات SQL injection، مادان[7] و همکارانش فرمولی برای ارزیابی مخاطره، ارائه دادهاند که از ۵ پارامتر پتانسیل

---

[1] LIKELIHOOD
[2] impact
[3] National Institute of Standards and Technology
[4] McGraw
[5] single loss expectancy
[6] Annualized rate of occurrence
[7] Madan

خرابی[1]، قابلیت تکثیر[2]، قابلیت استفاده[3]، کاربران مورد تأثیر[4] و قابلیت شناسایی[5] استفاده می‌کند[15]. شرکت سیسکو[6] برای ارزیابی مخاطرات در IPSهای سری ۴۲۰۰، از ۳ پارامتر شدت[7]، وفاداری[8] و نمره ارزش هدف[9] استفاده می‌کند[16].

کانوری فرمولی برای محاسبه مخاطرات حملات معروف شبکه ای، مانند سیل ریزی[10]، دستکاری[11]، جعل[12] و دیگر حملات رایج ارائه داده است[17]. این فرمول از ٤ پارامتر سختی شناسایی[13]، آسانی استفاده[14]، فراوانی[15] و تأثیر[16] استفاده می‌کند.

در این کتاب از فرمولی که کانوری برای ارزیابی مخاطره ارائه داده است، در ارزیابی مخاطرات پست الکترونیکی استفاده کرده‌ایم. پارامترهای مناسب و همچنین وزن دار بودن پارامترها، در این انتخاب نقش مهمی داشته است. پس از آن، به روزترین و جدیدترین مکانیزم‌های تأمین امنیت سرور و سیستم پست الکترونیکی را مورد بررسی قرار داده‌ایم و با انجام آزمایش‌هایی، میزان کاهش این مخاطرات را به صورت موردی بدست آورده‌ایم. در نهایت، پست الکترونیکی را از لحاظ مخاطره و سازمان‌ها دسته بندی کرده و با توجه به نتایج بدست آمده از فصل قبل، راهکارهای ایمن سازی ارائه داده‌ایم.

از آنجا که این کتاب، ترکیبی از مباحث مختلف در حوزه پست الکترونیکی و راهکارهای ایمن سازی سرور و سرویس پست الکترونیکی می‌باشد، می‌توان این کتاب را نگاهی جامع به مبحث امنیت در سرور و سرویس پست الکترونیکی دانست. البته کتاب‌ها و مقالاتی در این زمینه وجود دارد که هر یک وارد یک بحث جزئی از مباحث امنیت پست الکترونیکی شده‌اند.

---

[1] Damage Potential
[2] Reproducibility
[3] Exploitability
[4] Affected User
[5] Discoverability
[6] Cisco
[7] Sevirity
[8] Fidelity
[9] Target Value-Rating
[10] flooding
[11] manipulate
[12] spoof
[13] Detection difficulty
[14] Ease of Use
[15] Frequency
[16] Impact

به عنوان مثال در حوزه رمزنگاری[1] پست الکترونیکی، جین و همکارانش به تأمین امنیت پست پست الکترونیکی از طریق رمزنگاری و فشرده سازی[2]، راهکاری ارائه داده‌اند[18]. فارل بحثی در عدم نیاز به رمزنگاری پست الکترونیکی ارائه داده است[19]. در حوزه کرم‌های[3] پست الکترونیکی، زو مدلی برای کرم‌های پست الکترونیکی و مقابله با آن، ارائه داده است.[20] همچنین در حوزه spam، دآمبرا تحقیقاتی دارد و به مسائلی همچون لزوم پرداخت دولت‌ها به مبحث spam [21] و مقایسه سرعت تشخیص spam توسط انسان و رایانه می‌پردازد[22].

در این کتاب، پس از بررسی مخاطرات و ارائه فرمول و جدولی برای سنجش مخاطرات، به روش‌ها و مکانیزم‌های نوین تأمین امنیت و میزان کاهش درصد مخاطرات پرداخته‌ایم. در نهایت، راهکاری جامع برای تأمین امنیت سرور و سرویس پست الکترونیکی، ارائه داده‌ایم.

۱-۵ ساختار کتاب

ساختار این کتاب شامل ٦ فصل می‌باشد.

- فصل اول در مورد طرح مسئله، اهداف و کارهای مرتبط می‌باشد.
- فصل دوم به مفاهیم پایه ای می‌پردازد. نحوه عملکرد سیستم پست الکترونیکی بررسی می‌گردد و پروتکل‌های پست الکترونیکی من جمله pop3، imap، smtp و mime شرح داده می‌شوند. همچنین حملات را دسته بندی کرده و نتایج حملات را بررسی می‌کنیم.
- در فصل سوم، فرمول و جدول مخاطره ای ارائه می‌دهیم که از آن برای ارزیابی مخاطرات پست الکترونیکی، استفاده می‌کنیم. این فصل به مخاطرات پست الکترونیکی می‌پردازد، که شامل دو بخش مخاطرات در سرور پست الکترونیکی و مخاطرات در سرویس پست الکترونیکی می‌باشد. به مواردی همچون نا امن بودن سرور پست الکترونیکی، دستورات ناامن، عدم امنیت بسته[4]‌های پست الکترونیکی همچون sendmail، postfix و qmail، open relay، spam، ویروس‌ها، سرقت و خواندن داده‌ها، امن نبودن سرورهای pop3 و imap و فقدان امنیت webmail

---

[1] Encription
[2] Compressing
[3] Worms
[4] Package

اشاره می‌کنیم. برای بررسی مخاطرات، از جدول مخاطره و فرمولی که ارائه داده‌ایم، استفاده می‌کنیم.

- فصل چهارم، راهکارهای پیشنهادی برای رفع مخاطرات سرور و سرویس پست الکترونیکی را ارائه می‌دهد. در این فصل به مباحثی همچون امن کردن سرور پست الکترونیکی، امن کردن بسته‌های پست الکترونیکی من جمله postfix، sendmail و qmail، ممانعت از open relay، بلوکه کردن spam، فیلتر کردن ویروس، رله کردن گزینشی[1]، SASL، رمزنگاری داده‌ها توسط پروتکل‌هایی همانند SSL، TLS[2] و PGP[3]، استفاده از دیوارهای آتش[4] پست الکترونیکی، امن کردن سرورهای pop3 و imap و امن کردن webmail می‌پردازیم. با انجام آزمایش‌هایی، میزان کاهش این مخاطرات را به صورت موردی، توسط راهکارها و مکانیزم‌ها بررسی کرده‌ایم.
- فصل پنجم، به ارائه دسته بندی پست الکترونیکی و چگونگی ایمن سازی آنها و نتیجه گیری می‌پردازد.
- فصل ششم حاوی مراجع و منابع می‌باشد.

---

[1] Selective Relaying
[2] Transport Layer Security
[3] Pretty Good Protection
[4] Firewall

فصل دوم

مفاهیم پایه

این فصل به مفاهیم پایه ای می‌پردازد. نحوه عملکرد سیستم پست الکترونیکی، پروتکل‌های پست الکترونیکی من جمله pop3، imap، smtp و mime و همچنین سرآیندهای پست الکترونیکی شرح داده می‌شوند. در انتهای این فصل انواع حملات و نتایج آنها را بررسی می‌کنیم تا در فصل بعد از آن استفاده کنیم.

۲-۱ اصول پست الکترونیکی

در این قسمت به نحوه عملکرد سیستم پست الکترونیکی می‌پردازیم و اجزای مختلف این سیستم را بررسی می‌کنیم.

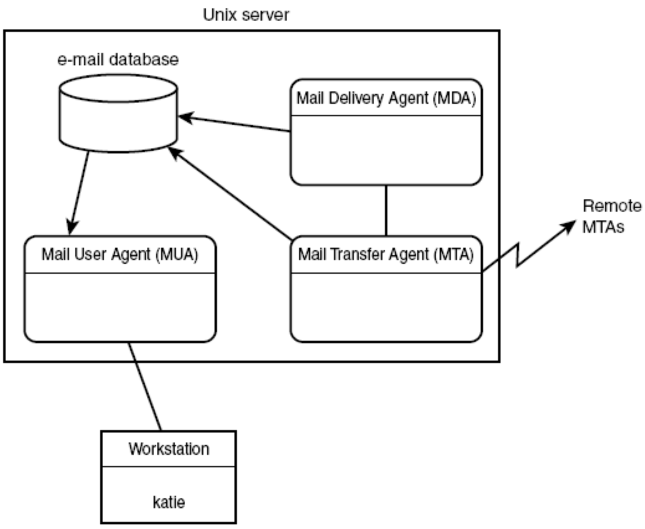
۲-۱-۱ سیستم‌های پست الکترونیکی لینوکسی[۱]

از دهه ۱۹۷۰ به بعد، سیستم عامل لینوکس به یکی از محبوب‌ترین سیستم عامل‌های دنیا تبدیل شد[2]. اکثر پست الکترونیکی سرورهای اینترنتی، از سرورهای لینوکسی استفاده می‌کنند.

یکی از مهم‌ترین ابداعات سیستم عامل لینوکس، ماژولار کردن نرم افزارهاست. بجای داشتن یک برنامه غول پیکر که کنترل کردن تمام قطعات مورد نیاز برای انجام یک کار را انجام می‌دهد، برنامه‌های کوچک‌تری ایجاد می‌شود تا با یکدیگر بتوانند کار کنند. هر برنامه قطعات کوچک‌تری را کنترل می‌کند تا تمام کار در نهایت انجام شود. این فلسفه در سیستم سرورهای پست الکترونیکی لینوکسی نیز استفاده می‌شود. وظایف پست الکترونیکی به چند قطعه تقسیم شده و به برنامه‌های مجزا تخصیص داده می‌شود. شکل ۲-۱ نشان می‌دهد که

[1] linux

چگونه اکثر سرورهای پست الکترونیکی متن باز[1]، وظایف پست الکترونیکی را در یک سیستم لینوکسی ماژوله بندی کرده اند.



شکل (۲-۱) : محیط ماژولار پست الکترونیکی در یونیکس

همان‌طور که در شکل ۲-۱ می‌بینید، یک سیستم پست الکترونیکی لینوکسی از سه بخش عمده زیر تشکیل شده است[23]:

- The Mail Delivery Agent (MDA)

- The Mail Transfer Agent (MTA)

- The Mail User Agent (MUA)

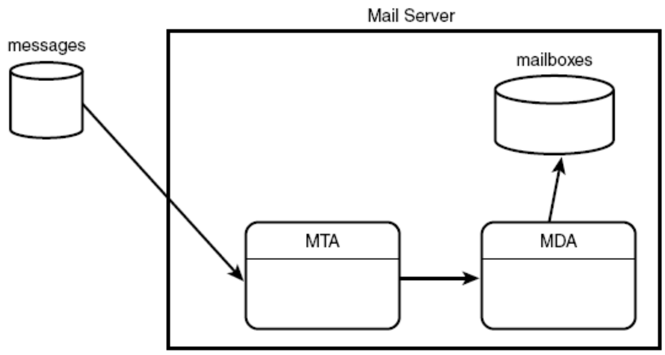
البته برخی از بسته‌های سرور پست الکترونیکی موجود، نقش MTA و MDA را تلفیق کرده‌اند و برخی دیگر نقش MDA و MUA را تلفیق کرده‌اند.

MDA

وظیفه MDA، تحویل دادن پیام‌ها به کاربران محلی می‌باشد[23]. MDA بر روی پیام‌هایی تمرکز دارد که مقصدشان، کاربر بر روی پست الکترونیکی سرور محلی می‌باشد. MDA

[1] Open Source

پیام‌ها را از MTA می‌گیرد، به MDA تحویل می‌دهد و تعیین می‌کند که پیام‌ها چگونه برسند.



شکل (۲-۲) : استفاده از MDA در سرور پست الکترونیکی

سه ویژگی عمده MDA عبارتند از:

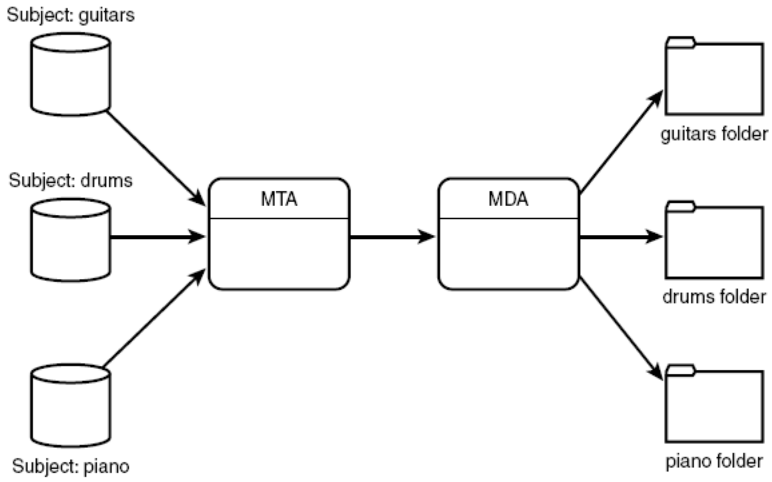
- فیلترگذاری خودکار پست الکترونیکی[1]
- پاسخگویی خودکار پست الکترونیکی[2]
- مقداردهی اولیه برنامه توسط پست الکترونیکی[3]

فیلترگذاری خودکار پست الکترونیکی

این قابلیت باعث می‌شود که درون پیام‌های ورودی جستجو کنیم و هنگامی که یک عبارت منطبق شد، پیام را درون پوشه خاصی در ناحیه پست الکترونیکی، ذخیره کنیم[23]. همچنین این قابلیت می‌تواند پیام‌های ناخواسته را فیلتر کند.

---

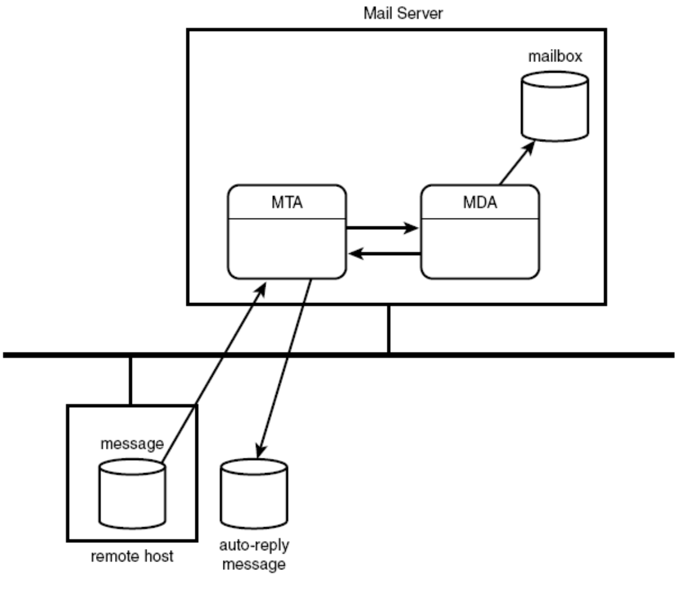
1 Automatic Mail Filtering
2 Automatic Mail Replying
3 Automatic Program Initialization By Mail



شکل (۲-۳) : فیلترگذاری خودکار پست الکترونیکی

پاسخگویی خودکار پست الکترونیکی

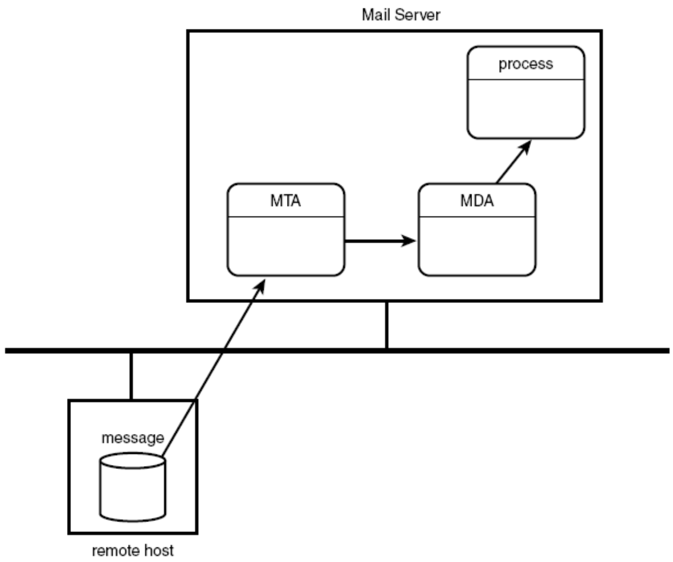
برنامه‌های MDA به کاربران پست الکترونیکی اجازه می‌دهند تا پیام‌های پاسخ را بر اساس سرآیند پیام، بفرستند[23].



شکل (۲-٤) : پاسخگویی خودکار پست الکترونیکی

مقداردهی اولیه برنامه توسط پست الکترونیکی

برنامه‌های MDA به کاربران پست الکترونیکی اجازه می‌دهند تا کاربران پست الکترونیکی، برنامه ای را بر اساس سرآیند پیام در یافتی، اجرا کنند[23].



شکل (۲-۵) : مقداردهی اولیه برنامه توسط پست الکترونیکی

MTA

MTA مسئول کنترل و تعامل با پیام‌های پستی ورودی و خروجی می‌باشد[23]. برای هر پیام پستی خروجی، MTA آدرس مقصد گیرنده را مشخص می‌کند. اگر مقصد، ماشین محلی باشد، MTA آن را به صندوق پستی[1] محلی یا MDA محلی، تحویل می‌دهد. ولی اگر مقصد سرور پست الکترونیکی راه دور[2] باشد، MTA یک اتصال با MTA راه دور، برقرار می‌کند. برای انتقال پیام‌ها، پروتکل‌های مختلفی استفاده می‌شود ولی رایج‌ترین آنها SMTP می‌باشد.

سه ویژگی عمده که یک MTA بایستی از آنها به خوبی پشتیبانی کند :

- امنیت
- آسانی پیکربندی

[1] mailbox
[2] remote

– سرعت پردازش پیام

معروف‌ترین بسته‌های پست الکترونیکی لینوکسی موجود، عبارتند از[2]:

- Sendmail
- Qmail
- Postfix

Sendmail محبوبیتش را به این خاطر بدست آورد که بسیار روان است. Qmail ایده برنامه پست الکترونیکی ماژولار را اخذ کرد و MTA خود را به صورت ماژولار نوشت. درQmail نیاز دارید که User-IDهای متفاوتی بر روی سرور پست الکترونیکی، اضافه کنید. هر ماژول، تحت یک User-id متفاوت، اجرا می‌شود. اگر نفوذ گر، یک ماژول را تحت سلطه خود در آورد، بر روی ماژول‌های دیگر، تأثیری نخواهد داشت. ویژگی امنیتی qmail، بهترین مزیت qmail محسوب می‌شود.

قابلیت اعتماد، ویژگی دیگر qmail می‌باشد. به صورتی که پیام موجود در صف پیام‌ها، گم نمی‌شود. همچنین qmail می‌تواند از ویژگی Maildir style بهره گیرد که از گم شدن و خراب شدن پیام‌ها جلوگیری می‌کند.

Qmail از فایل‌های پیکربندی گوناگون استفاده می‌کند که هر کدام برای یک ویژگی به وجود آمده اند. این مانع به وجود آمدن یک فایل پیکر بندی بزرگ می‌شود[12].

درPostfix نیاز دارید که User-IDهای متفاوت را بر روی سرور پست الکترونیکی، اضافه کنید. بر خلاف qmail که از User-Id مجزا، برای هر ماژول استفاده می‌کند، postfix هر ماژول را تحت یک user-id، اجرا می‌کند. بهر حال اگر نفوذ گری، یک ماژول را تحت سلطه خود در آورد، بر روی ماژول‌های دیگر، تأثیری نخواهد داشت.

یکی از بهترین ویژگی‌های postfix، سادگی آن است. بجای داشتن یک فایل پیکربندی پیچیده بزرگ یا فایل‌های پیکربندی فراوان کوچک، دو فایل پیکربندی وجود دارد که برای اجرا شدن، از کاربر پارامتر می‌گیرند[12].

در فصل مخاطرات، به شرح گسترده تری از این سه بسته پست الکترونیکی خواهیم پرداخت و مخاطرات آنها را بررسی می‌کنیم.

MUA

MUAها پیام‌ها را دریافت نمی‌کنند. آنها فقط پیام‌هایی را که در صندوق پستی کاربر هستند، نمایش می‌دهند[23]. همچنین بسیاری از MUAها، قابلیت ایجاد پوشه‌های متفاوت را برای ذخیره پیام‌ها، به کاربر می‌دهند.

تفاوت برنامه‌های MUA، بر دو اصل استوار است: محل ذخیره پیام‌ها و چگونگی نمایش پیام‌ها.

محل ذخیره پیام‌ها

دو فلسفه برای محل ذخیره سازی پیام‌ها وجود دارد[23]. فلسفه اول می‌گوید که وقتی کاربر پست الکترونیکی خود را می‌خواند، آن پیام از سرور بارگذاری[1] شده و بر روی سیستم کاربر قرار گیرد. اشکال کار این فلسفه این است که کاربر اگر از روی کامپیوتر دیگری، پست الکترونیکی خود را چک کند، چون پیام از روی سرور، حذف شده است قادر نخواهد بود پیام را بخواند. ولی خوبی این فلسفه این است که کار مدیر سیستم[2] را کم می‌کند. در فلسفه دوم پیام و پست الکترونیکی، از روی سرور پاک نمی‌شود و تنها یک کپی از آن به کاربر ارسال می‌شود و در این صورت، کاربر قادر است از روی هر کامپیوتری پست الکترونیکی خود را بخواند. ولی در عین حال، مشکل این روش، بار سنگینی است که بر روی دوش مدیر سیستم قرار می‌دهد.

چگونگی نمایش پیام‌ها

MUAها به گونه ای متفاوت با یکدیگر، پیام‌ها را نمایش می‌دهند[23]. برخی فقط به حالت متن ساده، پیام‌ها را نمایش می‌دهند. ولی برخی قابلیت نمایش بر اساس اسناد HTMLی که گرافیک را پشتیبانی می‌کنند، را نیز دارند. برای ایجاد این قابلیت بسیاری از MUAها، MIME را پشتیبانی می‌کنند. MIME این قابلیت را ایجاد می‌کند تا نسخه‌های مختلفی از پیام، وجود داشته باشد. در نهایت، کار MUA این است که MIME، پیام را نگاه می‌کند، اگر حالت متنی ساده باشد، آن را به خروجی متنی می‌دهد و اگر MIME، بیانگر حالت گرافیکی باشد، MUA آن را به خروجی گرافیکی، برای نمایش به کاربر می‌دهد.

[1] download
[2] administrator

۲-۱-۲ پروتکل‌های پست الکترونیکی

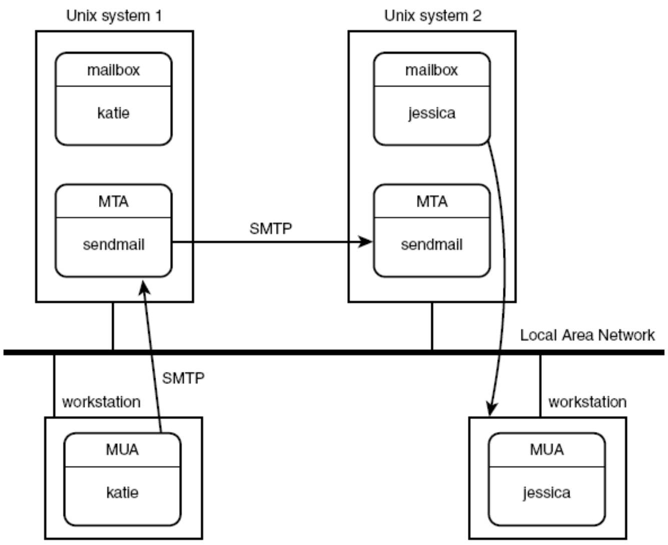
در قسمت‌های قبلی به معرفی MDA، MTA و MUA پرداختیم و وظیفه هر یک را بررسی کردیم. اکنون پروتکل‌های مورد استفاده در MDA، MTA و MUA را معرفی اجمالی کرده و شرح آنها را به قسمت‌های بعد کتاب موکول می‌کنیم.

پروتکل‌های MTA

برنامه‌های MTA بایستی قادر باشند با MTAهای راه دور دیگر، ارتباط برقرار کنند تا بتوانند پیام‌ها را منتقل کنند و همچنین اطلاعات مورد نیاز برای شناسایی پیام‌های راه دور را منتقل کنند. این کار توسط پروتکل smtp یا esmtp[1] انجام می‌گیرد.

پروتکل SMTP

پروتکل smtp به عنوان متد اولیه برای انتقال پیام‌ها در اینترنت، توسط سرورهای MTA ایجاد شد[25][24]. smtp از دستورات ساده ای برای ایجاد یک اتصال به MTA و انتقال اطلاعات و داده‌ها استفاده می‌کند. شکل ۲-٦ نمایشگر این مسئله است.



شکل (۲-۶) : اتصال smtp بین دو ایستگاه کاری

[1] Extended Simple Mail Transfer Protocol

پروتکل ESMTP

smtp اولیه که ایجاد شد حاوی نقایصی بود. برای رفع این نقایص، بجای ایجاد یک پروتکل جدید، پروتکل smtp را گسترش دادند و نام آن را ESMTP نهادند[26][27].

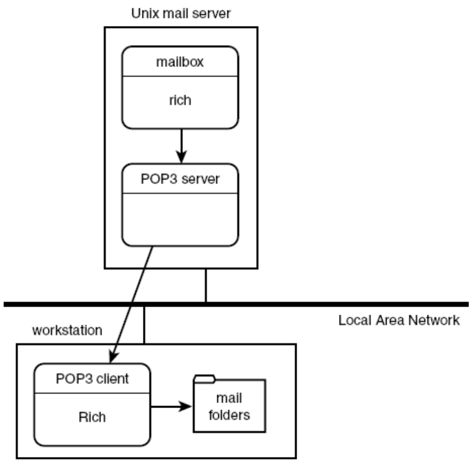
یک ویژگی مهم امنیتی آن است که ESMTP توانایی ورود[1] میزبان‌های MTA را به میزبان دریافتی می‌دهد. این مسئله در واقع، قابلیت تعیین هویت می‌باشد که درSMTP ESMTP اولیه وجود نداشت. این کار توسط دستورAUTH پیاده سازی شده است. کلاینت می‌تواند شناسه و گذرواژه خود را به سرور، برای تعیین هویت بدهد.

پروتکل‌های MUA

هدف پروتکل‌های MUA این است که به کاربران اجازه دهد پیام‌هایشان را، از صندوق پستی خود بخوانند.

پروتکل POP

ساده‌ترین پروتکل MUA، پروتکل POP می‌باشد. نسخه فعلیPOP، نسخه ۳ می‌باشد[9]. به طور معمول، وقتی از پروتکل POP استفاده می‌کنید، ایستگاه کاری MUA، پیام‌ها از روی صندوق پستی سرور، حذف می‌کند. بنابراین فضای زیادی از سرور پست الکترونیکی، پاک می‌شود. شکل ۲-۷ مثالی از اتصال POP3 را نشان می‌دهد.



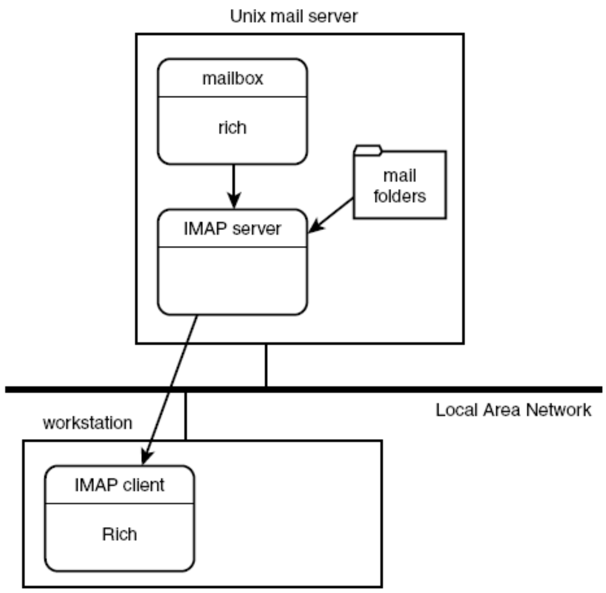
شکل (۲-۷) : مثالی از اتصال POP3

---

[1] Login

پروتکل IMAP

نسخه فعلی IMAP، نسخه ٤ می‌باشد[10]. در یک اتصال IMAP، تمامی پیام‌های پست الکترونیکی کاربر، بر روی سرور باقی می‌ماند. پیام‌ها فقط به این منظور بارگذاری می‌شوند که بتوان آنها را بر روی مانیتور ایستگاه کاری، نمایش داد. این پروتکل برای نمایش پیام‌ها از ایستگاه‌های کاری مختلف، مفید خواهد بود. فضای دیسک سرور پست الکترونیکی، بایستی به صورت دقیق مانیتور شود، چون در این پروتکل، پیام‌ها بر روی سرور باقی می‌مانند. شکل ۲-۸ مثالی از یک اتصال IMAP را نشان می‌دهد.



شکل (۲-۸) : مثالی از اتصال IMAP

۲-۲ پروتکل SMTP

در قسمت قبل به معرفی اجمالی پروتکل smtp پرداختیم. در اینجا به شرح بیشتری از این پروتکل خواهیم پرداخت.

Smtp برای رله کردن پیام‌ها و ضمیمه‌هایشان[1] به سیستم‌های کامپیوتری گوناگون، طراحی شده است[25][24]. استفاده از smtp، بسیار آسان است و پروتکل استانداردی است که برای انتقال پیام‌ها، در اینترنت استفاده می‌شود. Smtp از پورت ۲۵ tcp استفاده می‌کند.

۲-۲-۱ دستورات کلاینتی SMTP

این دستورات در جدول ۲-۱ فهرست شده‌اند[29][28].

جدول (۲-۱) : لیست دستورات کلاینتی smtp

دستور	توضیح
HELO	باز کردن خوش آمد گویی از طرف کلاینت
MAIL	شناسایی فرستنده پیام
RCPT	شناسایی گیرندگان
DATA	مشخص کردن شروع پیام
SEND	ارسال پیام به ترمینال
SQML	اجرای دستورات SEND یا MAIL
SAML	اجرای دستورات SEND و MAIL
RSET	راه اندازی مجدد اتصال SMTP
VRFY	تایید نام کاربری بر روی سیستم
EXPN	جستجو برای لیست و نام مستعار
HELP	لیستی از دستورات را درخواست می‌کند
NOOP	بدون عمل، هیچ کاری نمی‌کند
QUIT	جلسه SMTP را متوقف می‌کند
TURN	نقش‌های SMTP را معکوس می‌کند

[1] attachments

برخی از دستوراتی که از لحاظ امنیتی، حائز اهمیت هستند معرفی اجمالی کرده و در فصل مخاطرات، به بررسی مشکلات آنها می‌پردازیم.

دستور HELO: هدف دستور این است که کلاینت، خودش را به سرور smtp معرفی کند.

دستور SEND: این دستور به منظور ارسال پیام پست الکترونیکی مستقیم، به کاربری است که از طریق ترمینال login شده است.

دستور SQML: این دستور، همانند دستور send عمل می‌کند. اگر کاربر، login شده باشد، همانند send عمل می‌کند ولی اگر کاربر، login نشده باشد، پیام را به صندوق پستی گیرنده ارسال می‌کند.

دستور SAML: این دستور همانند دو دستور SEND و MAIL عمل می‌کند. این دستور هم به کاربر login شده، پیام می‌فرستد هم پیام را درون صندوق پستی کاربر، جای می‌دهد.

دستور VRFY: این دستور، صحت وجود کاربر گیرنده را مشخص می‌کند.

دستور TURN :هدف این دستور، برقراری ارتباط دوطرفه بین دو کامپیوتر در انتقال پیام، توسط یک اتصال tcp[1] می‌باشد.

۲-۲-۲ پاسخ‌های سرور

سرور در برابر دستور کلاینت، کدهایی از خود تولید می‌کند که نشانگر عمل انجام شده از سوی سرور، برای دستور صادر شده از سمت کلاینت است. این کدها در جداول زیر لیست شده‌اند[28][29].

[1] Transmission Control Protocol

جدول (۲-۲) : کدهای پاسخ خطای smtp

کد	توضیح
۵۰۰	خطای نحوی، فرمان شناخته شده نیست.
۵۰۱	خطای نحوی در پارامترها
۵۰۲	دستور پیاده سازی نشده است.
۵۰۳	دنباله بدی از دستورات
۵۰٤	پارامتر دستور، پیاده سازی نشده است.

جدول (۲-۳) : کدهای پاسخ اطلاعاتی smtp

کد	توضیح
۲۱۱	وضعیت سیستم یا کمک سیستم
۲۱٤	پیام کمک

جدول (۲-۴) : کدهای پاسخ سرویس smtp

کد	توضیح
۲۲۰	سرویس، آماده است
۲۲۱	سرویس، کانال انتقال را می‌بندد
٤۲۱	سرویس در دسترس نیست

جدول (۲-۵) : کدهای پاسخ عمل smtp

کد	توضیح
۲۵۰	پست الکترونیکی اقدام‌های درخواست شده درست، تکمیل شد.
۲۵۱	کاربر محلی وجود ندارد، به <forward-path> هدایت می‌شود.
۳۵٤	شروع ورودی پست الکترونیکی: پایان با <CR><LF><CR><LF>
٤۵۰	پست الکترونیکی اقدام‌های درخواست شده، گرفته نشده باشد: mailbox در دسترس نیست.
٤۵۱	درخواست عمل رد شده: اشکال در پردازش.
٤۵۲	عمل درخواست شده، گرفته نشده باشد: سیستم ذخیره سازی، کافی نیست.
۵۵۰	عمل درخواست شده، گرفته نشده باشد: جعبه پستی در دسترس نیست.
۵۵۱	کاربر محلی وجود ندارد: لطفاً <forward-path> را سعی کنید.
۵۵۲	عمل‌های پست الکترونیکی درخواست شده، رد شده است: تخصیص انباره، فراتر رفته است.
۵۵۳	عمل درخواست شده، گرفته نشده باشد: نام صندوق پستی، مجاز نمی‌باشد.
۵۵٤	تراکنش، از بین رفته است.

۲-۳ پروتکل‌های POP و IMAP

در قسمت قبل به معرفی اجمالی پروتکل‌های pop وimap پرداختیم. در اینجا به شرح بیشتر این پروتکل‌ها خواهیم پرداخت.

پروتکل POP3 از پورت TCP شماره ۱۱۰ بهره می‌برد[9]. پروتکل POP3 یکی از محبوب‌ترین پروتکل‌های خواندن پست الکترونیکی می‌باشد، ولی این پروتکل، نقص بزرگی دارد. هنگام خواندن پیام پست الکترونیکی توسط این پروتکل، پیام از سرور بارگذاری[1] شده، بر روی ایستگاه کاری[2] قرار می‌گیرد و از سرور حذف می‌شود. حال اگر کاربر از ایستگاه

[1] download
[2] workstation

کاری دیگری، مثلاً در محل کار بخواهد پیام‌هایش را بخواند، چون پست الکترونیکی از سرور حذف شده، قادر به خواندن پیام‌هایی که توسط ایستگاه کاری دیگری خوانده شده است، نمی‌باشد. ضمناً برخی از پیام‌ها، در روی یک ایستگاه کاری و برخی دیگر بر روی ایستگاه کاری دیگری قرار گرفته‌اند. البته این پروتکل به حفظ و کاهش فضای دیسک سرور، کمک شایانی می‌کند.

پروتکل imap برای رفع نقیصه پروتکل POP3 به وجود آمد[10]. این پروتکل بدین صورت عمل می‌کند که صندوق پستی[1] بر روی سرور قرار دارد و هر کاربری که در خواست خواندن پست الکترونیکی خود را دارد، یک کپی از پیام پست الکترونیکی موجود بر روی سرور، برایش ارسال می‌شود و پیام بر روی سرور باقی می‌ماند. بدین صورت، کاربر از هر ایستگاه کاری می‌تواند پیام پست الکترونیکی خود را بخواند و دودستگی در پست الکترونیکی، به وجود نخواهد آمد. البته در این پروتکل، مراقبت از فضای دیسک و مدیریت آن، اهمیت زیادی دارد که در پروتکل POP3، این مسئله وجود نداشت. شماره پورتی که IMAP استفاده می‌کند ۱۴۳ می‌باشد.

۲-۴ MIME

همان‌طور که گفته شد، پروتکل SMTP برای ارسال داده‌ها، از دستور DATA که داده‌ها را به صورت متن ASCII[2] ارسال می‌کند، استفاده می‌کند[26]. حال سؤال این است که چگونه می‌توان عکس، نوشته ای به زبان چینی و یا چند رسانه ای را ارسال کرد؟ پاسخ ساده است: در اینجا داده‌های باینری، در طول پروسه ارسال پست الکترونیکی به فرمت متن ASCII تبدیل می‌شوند و در مقصد عمل عکس صورت می‌گیرد، یعنی متن ASCII به داده باینری، مانند عکس و ... تبدیل می‌شود.

در این قسمت متدهایی را بررسی می‌کنیم که برای انتقال داده باینری، به سرورهای پست الکترونیکی راه دور استفاده می‌شود. به بررسی دو متد Uuencode و MIME می‌پردازیم.

---

[1] mailbox

[2] American Standard Code for Information Interchange

۲-۴-۱ برنامه Uuencode

سال‌ها پیش، قبل از به وجود آمدن smtp، کاربرانی که با یونیکس[1] کار می‌کردند، داده‌های به فرمت باینری را به فرمت اسکی تبدیل می‌کردند. آنها از متد uuencode برای این کار استفاده می‌کردند[2]. uu در این عبارت، همان Unix to Unix می‌باشد که بخشی از پروتکل UUCP[2] است تا انتقال داده‌ها را میان کامپیوترهای لینوکسی، با استفاده از dial-up و مودم‌های اختصاصی، فراهم سازد. بسیاری از بسته‌های smtp، از این متد برای ارسال داده باینری استفاده می‌کنند. البته در بسته‌های جدید، این متد غیر فعال شده است.

uuencode از شمای کدگذاری ۳ به ٤ استفاده می‌کند. یعنی ۳ بایت باینری[3]، به ٤ بایت اسکی تبدیل می‌شوند[2]. این الگو به صورت چشمگیری، حجم فایلی را که خواهان انتقال آن هستیم، افزایش می‌دهد. برای همین فایل باینری را قبل از کدگذاری، فشرده می‌کنیم.

۲-۴-۲ MIME و داده‌های باینری

علت اینکه بسته‌های جدید پست الکترونیکی، از uuencode استفاده نمی‌کنند این است که پروتکل استاندارد اینترنتی MIME، برای کدگذاری داده‌های باینری ایجاد شد[30]. MIME بسیار متنوع‌تر از uuencode در زمینه ارسال اطلاعات اضافه، درباره فایل به کدگشا[4] می‌باشد، که باعث می‌شود کدگشا، انواع مختلفی از فایل‌های باینری را بشناسد و کدگشایی کند.

۲-۴-۳ فیلدهای سرآیند MIME

MIME، ٥ فیلد سرآیند، به پیام اضافه می‌کند که باعث شناسایی چگونگی کدگذاری فایل باینری می‌شود[30]. در جدول ۲-٦، این سرآیندها را مشاهده می‌کنید.

[1] unix
[2] Unix to Unix Copy
[3] binary
[4] decoder

جدول (۲-٦) : فیلدهای سرآیند پیام MIME

فیلد	توضیح
MIME-Version	نسخه MIME استفاده شده را نمایش می‌دهد
Content-Transfer-Encoding	مشخص کردن طرح رمزگذاری استفاده شده، برای رمز کردن داده‌های باینری به اسکی.
Content-ID	مشخص کردن شناسه منحصر به فرد، برای بخش پیام.
Content-Description	توضیح کوتاهی برای بخش پیام.
Content-Type	تعیین نوع مطالب موجود در داده‌های کد گذاری شده.

فیلد Content-Transfer-Encoding

این فیلد نشان می‌دهد که داده باینری موجود در پیام چگونه کدگذاری می‌شود[30]. هفت متد مختلف برای این کار وجود دارد که در جدول ۲-۷ نشان داده شده است.

جدول (۲-۷) : متدهای کدگذاری MIME [30]

متد	توضیح
7-bit	متن اسکی ۷ بیتی استاندارد
8-bit	متن اسکی ۸ بیتی استاندارد
binary	داده باینری خام
Quoted-printable	داده‌ها را به کاراکترهای قابل چاپ در مجموعه کاراکترهای اسکی، کدگذاری می‌کند.
Base64	٦ بیت باینری داده را به ۸ بیت کاراکتر قابل چاپ، کدگذاری می‌کند.
Ietf token	کدگذاری توکن گسترش پذیر که با یک RFC نشان داده شده است.
x-token	دو کاراکتر -X یا -x بدون فاصله، با هر توکن دیگر

سه متد اول، هیچ کدگذاری بر روی داده انجام نمی‌دهد. بیشترین متدی که برای کدگذاری داده باینری استفاده می‌شود، متد base64 است که داده‌های باینری را توسط نگاشت بلوک‌های ٦ بیتی داده‌های باینری، به اسکی‌های ۸ بیتی کدگذاری می‌کند. جدول ۲-۸ این نگاشت را نشان می‌دهد[30].

جدول (۲-۸) : متد کدگذاری base64

Value Encoding	Value Encoding	Value Encoding	Value Encoding
0 A	17 R	34 i	51 z
1 B	18 S	35 j	52 0
2 C	19 T	36 k	53 1
3 D	20 U	37 l	54 2
4 E	21 V	38 m	55 3
5 F	22 W	39 n	56 4
6 G	23 X	40 o	57 5
7 H	24 Y	41 p	58 6
8 I	25 Z	42 q	59 7
9 J	26 a	43 r	60 8
10 K	27 b	44 s	61 9
11 L	28 c	45 t	62 +
12 M	29 d	46 u	63 /
13 N	30 e	47 v	(pad) =
14 O	31 f	48 w	
15 P	32 g	49 x	
16 Q	33 h	50 y	

فیلد Content-Type

این فیلد حاوی ۲ قسمت است[30] که به صورت زیر مشخص می‌شود:

Content-Type: type /subtype

قسمت type، فرمت محتوای کلی را مشخص می‌کند و subtype نیز فرمت محتوای خاص را مشخص می‌کند. Type به ۷ دسته زیر تقسیم می‌شود.

text

message

image

video

audio

application

multipart

Multipart Content-Type

این نوع محتوا، نوع مخصوصی است و پیام‌هایی را مشـخص مـی‌کنـد کـه چنـد نـوع مختلـف محتوا، درون یک پیام قرار دارند[30]. این نوع باعث می‌شود که پیام را به اشـکال گونـاگون، مانند ascii/text، html و فرمت صدادار نمایش داد. توسط شناسه boundary می‌توان چنـد نوع را معرفی نمود. در واقع مرز بین انواع مختلف را نشان می‌دهد که دسـتورات smtp زیـر این مسئله را نشان می‌دهد:

MIME-Version: 1.0

Content-Type: multipart/alternative; boundary=bounds1

--bounds1

Content-Type: text/plain; charset=us-ascii

This is the plain text part of the message that can be read by simple

e-mail readers.

--bounds1

Context-Type: text/enriched

This is the <bold>rich text</bold> version of the <bigger>SAME</bigger>

message.

--bounds1--

۲-۵ دسته بندی حملات

اغلب نمی‌توان حملات را به شکل دقیقی دسته‌بندی کرد. اکثر دسته‌بندی‌ها به گونه‌ای هستند که یک حمله، یا در دسته ای قرار می‌گیرد، یا در هیچ دسته ای قرار نمی‌گیرد[17]. با این وجود، دسته بندی حملات، برای این کتاب لازم و ضروری است، چون در فصول بعدی برای

مخاطرات، جداولی را سازماندهی کرده‌ایم که مبنای کار می‌باشد و همچنین در حوزه امنیت، بدون در اختیار داشتن یک دسته بندی جامع از حملات امنیتی، نمی‌توان تشخیص داد که آیا آن طرح ایمن است یا خیر. برای همین با مطالعه و کار بر روی حملات موجود، دسته‌های[1] اصلی زیر را ارائه داده‌ایم:

خواندن[2] – دسترسی غیر مجاز به اطلاعات

دستکاری[3] – تغییر اطلاعات

جعل[4] – ارائه اطلاعات یا خدمت غلط

سیل ریزی[5] – سرریز منابع یک کامپیوتر

هدایت[6] – تغییر جریان اطلاعات

ترکیبی[7] – استفاده از چند روش فوق

۲-۶ نتایج حمله

هر حمله نتیجه ای در بر دارد. نتایج حمله را به ۵ دسته کلی تقسیم بندی می‌کنیم[17]:

- افشای اطلاعات[8]: عبارتست از، انتشار اطلاعات بین افرادی که مجاز به دسترسی به به آن نیستند. این شامل دزدی گذرواژه، خواندن بخش‌های غیر مجاز از دیسک سخت، آموختن اطلاعات محرمانه قربانی و نظایر آن است.
- تخریب اطلاعات[9]: عبارتست از تغییر غیر مجاز اطلاعات ذخیره شده یا در حال انتقال. مثال‌هایی از این دست عبارتند از: تغییر شکل[10] سایت‌های وب، حملات مرد میانی[1]و ویروس‌هایی که داده‌ها را خراب می‌کنند.

---

1 Categories
2 Read
3 manipulate
4 spoof
5 flood
6 redirect
7 composite
8 Disclosure of information
9 Corruption of information
10 defacement

- منع خدمت[2]: عبارتست از کاهش یا مسدود سازی عمدی منابع شبکه. اغلب حملات سیل ریزی[3]، با هدف منع خدمت اجرا می‌شوند.
- دزدی خدمت[4]: عبارتست از دسترسی غیر مجاز به خدمات کامپیوتر یا شبکه، بدون تنزل دادن خدمات به کاربران عادی. مثال‌هایی از این دست عبارتند از: دزدی گذرواژه و ورود به شبکه، دسترسی به LAN بی سیم بدون مجوز و دزدی نرم‌افزار.
- دسترسی بیشتر: عبارتست از افزایش غیر مجاز حقوق دسترسی به یک کامپیوتر یا شبکه. اجرای یک حمله سرریز بافر[5] نمونه خوبی از حملاتی است که سبب دسترسی بیشتر می‌شود.

[1] Man in the middle
[2] Denial of service
[3] flooding
[4] Theft of service
[5] Buffer overflow

فصل سوم

مخاطرات

این فصل، به مخاطرات پست الکترونیکی می‌پردازد که شامل دو بخش مخاطرات در سرور پست الکترونیکی و مخاطرات در سرویس پست الکترونیکی می‌باشد. به مواردی همچون ناامن بودن سرور پست الکترونیکی، دستورات ناامن، عدم امنیت بسته[1]های پست الکترونیکی همچون sendmail، postfix و qmail، open relay، spam، ویروس‌ها، سرقت و خواندن داده‌ها، امن نبودن سرورهای pop3 و imap و فقدان امنیت webmail می‌پردازیم. هر یک از مخاطرات ارائه شده را با جدول مخاطره و فرمولی که ارائه می‌دهیم، بررسی می‌کنیم. راهکارهای ایمن سازی در فصل بعد ارائه می‌شود.

۳-۱ ارزیابی مخاطرات سیستم‌های پست الکترونیکی

با بررسی صورت گرفته، در حوزه مخاطرات سیستم‌های پست الکترونیکی و ارزیابی آن، روش خاصی ارائه نشده است، اما در حوزه مخاطرات سیستم‌های دیگر، تحقیقاتی صورت گرفته و روش‌هایی ارائه شده است.

استون برنر و همکارانش، در حوزه مخاطرات سیستم‌های بر مبنای IT، فرمولی ارائه داده‌اند که بسیاری از افراد در ارزیابی مخاطرات، از آن استفاده می‌کنند. فرمول از دو پارامتر احتمال کلی[2] و تأثیر[3] استفاده می‌کند[13]. این فرمول در قالب توصیه نامه ای از سازمان NIST[4] ارائه شده است و افراد مختلف با تغییر نام پارامترها، آن را به همان شیوه استفاده می‌کنند. برای مثال در حوزه امنیت نرم افزار و شبکه، مک گراو[5] فرمولی ارائه داده است که از دو پارامتر انتظار کاهش تنها[6] و نرخ رخداد در سال[1] برای محاسبه مخاطره استفاده

---

[1] Package
[2] LIKELIHOOD
[3] impact
[4] National Institute of Standards and Technology
[5] McGraw
[6] single loss expectancy

می‌کند [14]. این در واقع، همان پارامترهای تغییر نام یافته ای است که در فرمول ارائه شده از سوی استون برنر و همکارانش، ذکر شد.

البته افرادی وجود دارند که از فرمول‌های دیگر و پارامترهای اضافه تری استفاده کرده‌اند. برای مثال در حملات SQL injection، مادان[2] و همکارانش، فرمولی برای ارزیابی مخاطره ارائه داده‌اند که از ٥ پارامتر پتانسیل خرابی[3]، قابلیت تکثیر[4]، قابلیت استفاده[5]، کاربران مورد تأثیر[6] و قابلیت شناسایی[7] استفاده می‌کند[15]. شرکت سیسکو[8] برای ارزیابی مخاطرات در IPSهای سری ٤٢٠٠، از ٣ پارامتر شدت[9]، وفاداری[10] و نمره ارزش هدف[11] استفاده می‌کند[16].

کانوری فرمولی برای محاسبه مخاطراتی حملات معروف شبکه ای، مانند سیل ریزی[12]، دستکاری[13]، جعل[14] و دیگر حملات رایج ارائه داده است[17]. این فرمول از ٤ پارامتر سختی شناسایی[15]، آسانی استفاده[16]، فراوانی[17]و تأثیر[18] استفاده می‌کند. در این کتاب از فرمولی که کانوری برای ارزیابی مخاطره ارائه داده است، در ارزیابی مخاطرات پست الکترونیکی استفاده کرده‌ایم. پارامترهای مناسب و همچنین وزن دار بودن پارامترها، در این انتخاب نقش مهمی داشته است.

---

[1] Annualized rate of occurrence
[2] Madan
[3] Damage Potential
[4] Reproducibility
[5] Exploitability
[6] Affected User
[7] Discoverability
[8] Cisco
[9] Sevirity
[10] Fidelity
[11] Target Value-Rating
[12] flooding
[13] manipulate
[14] spoof
[15] Detection difficulty
[16] Ease of Use
[17] Frequency
[18] Impact

۳-۱-۱ احتمال کلی و تأثیر

همان‌طور که ذکر شد، بسیاری از افراد همانند استون برنر و مک گراو، از دو پارامتر احتمال کلی و تأثیر برای ارزیابی مخاطره استفاده می‌کنند[13]. نرخ مخاطره بدست آمده این گونه محاسبه می‌شود:

نرخ مخاطره = احتمال کلی * تأثیر

نقطه قوت این گونه ارزیابی این است که یک روش کلی ارزیابی می‌باشد و بسیاری از افراد از آن استفاده می‌کنند.

نقاط ضعف این گونه ارزیابی مخاطره، در سیستم‌های پست الکترونیکی عبارتند از:

– پارامترهایی در ارزیابی مخاطره، در نظر گرفته نشده‌اند که برای ارزیابی مخاطرات در سیستم‌های پست الکترونیکی حایز اهمیت هستند.

– میزان اثر پارامترها و ضریب پارامترها در ارزیابی، یکسان در نظر گرفته شده است که این مسئله برای ارزیابی مخاطرات پست الکترونیکی مناسب نمی‌باشد.

۳-۱-۲ روش‌های دیگر

در ارزیابی دیگران از مخاطرات، همان‌گونه که ذکر شد افراد مختلف فرمول‌های خاصی ارائه داده‌اند. برای مثال در حملات SQL injection، مادان[1] و همکارانش فرمولی برای ارزیابی مخاطره ارائه داده‌اند که از ۵ پارامتر پتانسیل خرابی[2]، قابلیت تکثیر[3]، قابلیت استفاده[4]، کاربران مورد تأثیر[5] و قابلیت شناسایی[6] استفاده می‌کند[15]. شرکت سیسکو[7] برای ارزیابی ارزیابی مخاطرات در IPSهای سری ۴۲۰۰، از ۳ پارامتر شدت[8]، وفاداری[1] و نمره ارزش هدف[2] استفاده می‌کند[16].

---

[1] Madan
[2] Damage Potential
[3] Reproducibility
[4] Exploitability
[5] Affected User
[6] Discoverability
[7] Cisco
[8] Sevirity

نقطه قوت این روش‌های ارزیابی برای پست الکترونیکی در آن است که از پارامترهای بیشتری بهره برده‌اند. نقطه ضعف در آن است که میزان اثر پارامترها و ضریب پارامترها، در ارزیابی، یکسان در نظر گرفته شده است و این مسئله برای ارزیابی مخاطرات پست الکترونیکی، مناسب نمی‌باشد. البته قابل ذکر است که این روش‌ها در جای خود، کارایی دارند ولی برای سیستم‌های پست الکترونیکی، کارایی ندارند.

۳-۱-۳ روش کانوری

با توجه به موارد ذکر شده، نیاز به فرمولی است که سه ویژگی زیر را دارا باشد:

- دو پارامتر اصلی احتمال کلی و تأثیر را دارا باشد، مطابق با توصیه نامه NIST باشد و از روش کلی تبعیت کند.
- پارامترهای اضافه تری که در ارزیابی مخاطرات سیستم‌های پست الکترونیکی حائز اهمیت هستند را، دارا باشد.
- پارامترها، دارای وزن و ضریب باشند چون میزان تأثیر پارامترها در ارزیابی مخاطرات پست الکترونیکی، یکسان نیستند.

کانوری فرمولی برای محاسبه مخاطرات حملات معروف شبکه ای، مانند سیل ریزی[٣]، دستکاری[٤]، جعل[٥] و دیگر حملات رایج، ارائه داده است[17]. این فرمول از ٤ پارامتر سختی شناسایی[٦]، آسانی استفاده[٧]، فراوانی[٨] و تأثیر[٩] استفاده می‌کند. در این تحقیق از فرمولی که کانوری برای ارزیابی مخاطره به کاربرده است، در ارزیابی مخاطرات پست الکترونیکی استفاده کرده‌ایم.

پارامترهای مناسب، نزدیک بودن مخاطرات پست الکترونیکی به مخاطرات بررسی شده توسط کانوری، تبعیت از روش ارائه شده کلی توسط NIST و همچنین وزن دار بودن

---

[1] Fidelity
[2] Target Value-Rating
[3] flooding
[4] manipulate
[5] spoof
[6] Detection difficulty
[7] Ease of Use
[8] Frequency
[9] Impact

پارامترها در این انتخاب، نقش مهمی داشته است. فرمول ارائه شده برای ارزیابی، به صورت زیر می‌باشد.

جمع امتیاز = **سختی شناسایی** + (**آسانی استفاده***۲) + (**فراوانی***۳) + (**تأثیر***۴)

محدوده اعداد سختی شناسایی، آسانی استفاده، فراوانی و تأثیر بین ۱ الی ۵ می‌باشد. جمع امتیاز بدست آمده، بین ۱ تا ۵۰ می‌باشد. اما اینکه این ٤ پارامتر نشان دهنده چه مسئله ای می‌باشند:

- سختی شناسایی: به طور تقریبی نشان دهنده دشواری کشف حمله، توسط کارکنان شبکه است. فرض شده است مهاجم توانایی متوسطی دارد.
- آسانی استفاده: نشان دهنده سادگی اجرای حمله است.
- فراوانی: نشان دهنده آن است که حمله، هر چند وقت یک‌بار انجام می‌شود.
- تأثیر: معیاری از آسیبی که اجرای موفقیت آمیز حمله، به شبکه وارد می‌کند[17].

۳-۱-۴ عناصر جدول ارائه شده

جدولی برای هر مخاطره تشکیل شده و فرمول در آن بکار رفته است، تا روند ارزیابی را تسهیل بخشد. این جدول در ارائه نتیجه گیری، بسیار حائز اهمیت می‌باشد. اعداد موجود در جداول، در واقع مطالعه موردی می‌باشد و بر اساس تجربیات می‌باشد. بدست آوردن دقیق این اعداد برای هر مخاطره پست الکترونیکی، می‌تواند موضوع تحقیقات بعدی باشد و افراد بر آن مطالعه کنند. تست انجام شده بر روی سرور پست الکترونیکی Qmail، انجام شده است. در فصل‌های بعدی از این جدول و فرمول استفاده خواهد شد. نمونه ای از جدول را برای مخاطره spam مشاهده می‌کنید.

جدول(۳-۹) : جدول مخاطره spam

نام مخاطره	مخاطره spam
دسته حملات مرتبط با مخاطره	سیل ریزی – جعل
چگونگی استفاده	با ارسال حجم زیاد اطلاعات، باعث از کار افتادن سرور پست الکترونیکی می‌شود – در پست الکترونیکی، خود را فرد دیگری معرفی کرده، با راه‌های مهندسی اجتماعی، از فرد سوء استفاده کرده و او را به مقصد دلخواه می‌کشاند.
نتیجه حملات	منع خدمت– افشای اطلاعات
حملات بعدی	دزدی خدمت– دسترسی بیشتر
شناسایی و محافظت	بلوکه کردن پیام‌هایی که از میزبان‌های spam شناخته شده می‌آید -بلوکه کردن پیام‌هایی که محتوی subject header تجاری شناخته شده، هستند – بلوکه کردن پیام‌هایی که در پایگاه داده spam جهانی لیست شده‌اند.
سختی شناسایی	٤
آسانی استفاده	٤
فراوانی	٥
تأثیر	٤
جمع امتیاز	٤٣

جمع امتیاز = سختی شناسایی + (آسانی استفاده*۲) + (فراوانی*۳) + (تأثیر*۴)

محدوده اعداد سختی شناسایی، آسانی استفاده، فراوانی و تأثیر بین ۱ الی ۵ می‌باشد. جمع امتیاز بدست آمده بین ۱ تا ۵۰ می‌باشد. اما اینکه این ٤ پارامتر، نشان دهنده چه مسئله ای می‌باشند[17]:

- سختی شناسایی: به طور تقریبی، نشان دهنده دشواری کشف حمله، توسط کارکنان شبکه است. فرض شده است مهاجم توانایی متوسطی دارد.
- آسانی استفاده: نشان دهنده سادگی اجرای حمله است.
- فراوانی: نشان دهنده آن است که حمله هر چند وقت یک‌بار، انجام می‌شود.
- تأثیر: معیاری از آسیبی که اجرای موفقیت آمیز حمله، به شبکه وارد می‌کند.

۳-۲ مخاطرات سرور پست الکترونیکی

اگر سرور پست الکترونیکی امن نباشد، نفوذ گر با نصب درب‌های پشتی[1] روی سیستم، باعث باعث به خطر افتادن سیستم و از کار افتادن سرویس پست الکترونیکی می‌شود[12]. در این قسمت به مخاطرات سرور پست الکترونیکی می‌پردازیم.

۳-۲-۱ مخاطرات سرورهای خانواده یونیکس[2]

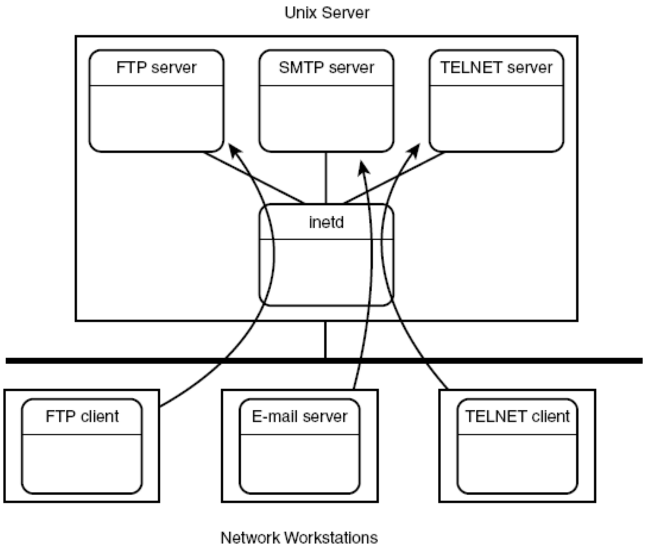
با توجه به اینکه اکثر سرورهای محبوب مانند gmail، yahoomail و ... از سرورهای لینوکسی استفاده می‌کنند[12]، مخاطرات سرورهای خانواده یونیکس را بررسی می‌کنیم.

حملات شبکه ای[3]

برنامه inetd یک برنامه شبکه ای مستقل می‌باشد که به تمام درخواست‌های شبکه ای که از کلاینت‌های راه دور رسیده است، گوش می‌دهد. اگر یک اتصال شناسایی شود، inetd برنامه مورد نظر را راه اندازی کرده و اتصال را، تحویل آن برنامه می‌دهد.

---

[1] backdoor
[2] unix
[3] Network attacks



شکل (۳-۱) : برنامه لینوکسی inetd

برنامه inetd منبع حملات شبکه ای بسیار فراوان می‌باشد، بنابراین امن کردن این برنامه از کارهایی است که بایستی صورت گیرد[32].

دسترسی شبکه ای

اگر به سرور به هر نحوی دسترسی پیدا شود و درب پشتی بر روی سیستم نصب شود، می‌تواند بسیار خطرناک باشد. به همین دلیل بایستی مکانیزم‌هایی ارائه دهیم تا اگر به سرور، دسترسی ایجاد شد، با اقدامات آن مقابله کنیم.

جدول (۳-۱) : مخاطره حملات شبکه ای و دسترسی شبکه ای

نام مخاطره	حملات شبکه ای و دسترسی شبکه ای
دسته حملات مرتبط با مخاطره	خواندن – دست‌کاری- سیل ریزی
چگونگی استفاده	متصل شدن به سرویس شبکه ای که نباید فعال باشد و سوء استفاده از آن – استفاده از درب‌های پشتی
نتیجه حملات	افشای اطلاعات - تخریب اطلاعات- منع خدمت
حملات بعدی	دزدی خدمت - دسترسی بیشتر
شناسایی و محافظت	ایمن سازی inetd – نصب فایروال و IPS و IDS
سختی شناسایی[1]	۳
آسانی استفاده[2]	۳
فراوانی[3]	۲
تأثیر[4]	۵
جمع امتیاز[5]	۳۵

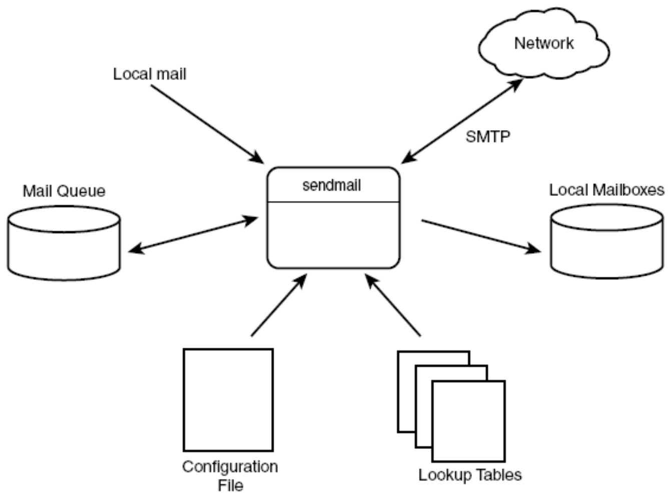
[1] Detection Difficulty
[2] Ease of use
[3] Frequency
[4] Impact
[5] Overall rating

۳-۲-۲ مخاطرات بسته‌های پست الکترونیکی Sendmail، Qmail و Postfix

پس از بررسی اجمالی بسته‌های پست الکترونیکی Sendmail، Qmail و Postfix و نحوه کارکرد آنها، به بررسی مخاطرات موجود در این بسته‌های پست الکترونیکی خواهیم پرداخت.

بسته پست الکترونیکی Sendmail

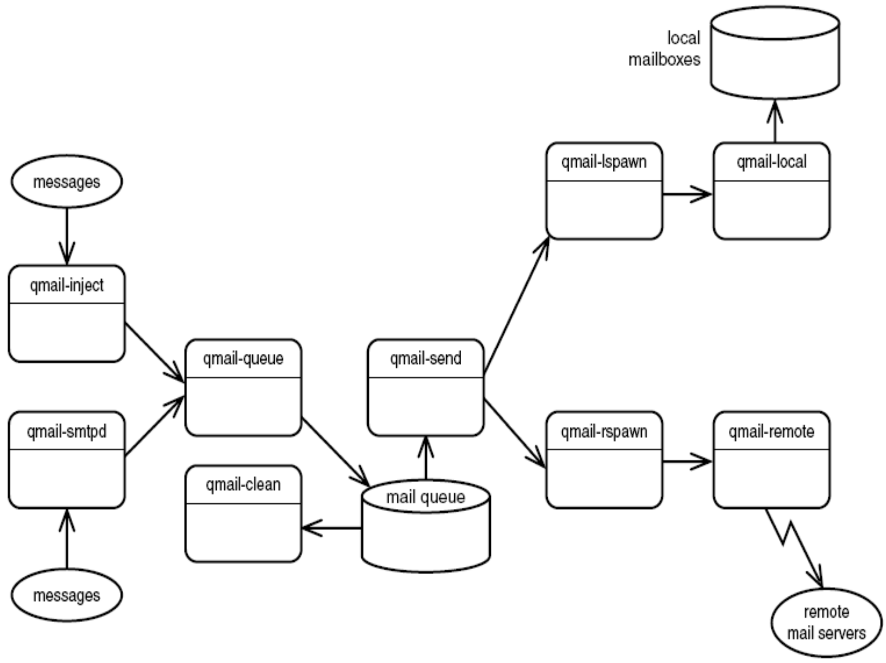
بسته پست الکترونیکی sendmail، در سالیان پیش، شامل حفره‌های امنیتی بود ولی درسال‌های اخیر بازنویسی شد و ویژگی‌های بسیاری از جمله ویژگی‌های امنیتی، به آن اضافه شد. در نسخه‌های جدید، ثابت شده است که این بسته، بسیار امن می‌باشد[33]. در شکل ۳-۲ قسمت‌های مختلف بسته sendmail، نشان داده شده است.



شکل (۳-۲) : بلاک دیاگرام sendmail

بسته پست الکترونیکی Qmail

Qmail چیزی بیش از یک جایگزین ساده برای Sendmail می‌باشد. Qmail تفاوت‌های زیادی با Sendmail دارد. Qmail از برنامه‌های اجرایی متعددی که با هم برای ارسال پیام در تعاملند، تشکیل شده است. همچنین Qmail فایل‌های متنی بسیار فراوانی برای پیکربندی فایل‌های اجرایی خود دارد[34]. شکل ۳-۳ بلوک دیاگرام بسته پست الکترونیکی Qmail را نشان می‌دهد.



شکل (۳-۳) : بلاک دیاگرام Qmail

۹ برنامه اصلی در qmail وجود دارد[34]. Qmail queue پیام‌ها را در صف پست الکترونیکی، ذخیره می‌کند. دو برنامه بعدی، پیام‌ها را وارد qmail queue می‌کنند. Qmail inject به صورت محلی و qmail smtpd برای ارسال پیام‌ها، از پست الکترونیکی سرورهای راه دور، عمل می‌کند. پس از اینکه پیام‌ها به خوبی در qmail queue ذخیره شدند، برنامه qmail send صدا زده می‌شود که وظیفه تحویل پیام‌ها به مقصد مناسب را داراست. پیام‌هایی که به عنوان پیام‌های محلی برای پست الکترونیکی سرور شناخته می‌شوند، به qmail-lspawn تحویل داده می‌شوند و پیام‌هایی که به عنوان پیام‌های راه دور برای پست الکترونیکی سرور، شناخته می‌شوند، به qmail-rspawn تحویل داده می‌شوند. برنامه qmail-clean، هر پیغامی که درون qmail-queue باقی مانده است را پاک می‌کند. چون آن پیام‌ها به عنوان پیام‌هایی شناخته شده‌اند که وضعیت مشخصی ندارند و به عنوان پیام‌هایی که به هیچ وجه قابل تحویل نیستند، علامت خورده‌اند. هر دو برنامه qmail-lspawn و qmail-rspawn، برنامه‌های کمکی به صورت مجزا دارند. هر کدام از این برنامه‌ها، به تحویل پیام به مقصد مناسب، کمک می‌کند.

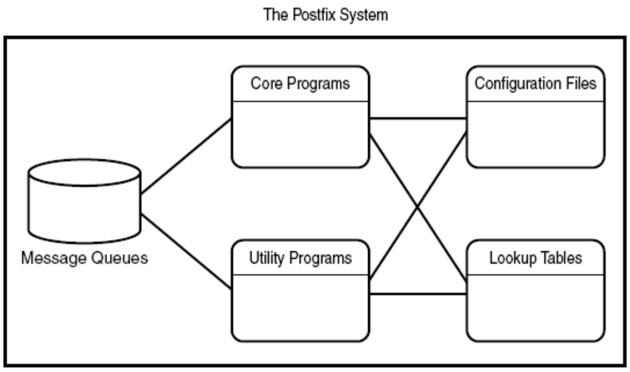
همان‌طور که گفته شد، qmail فایل‌های پیکر بندی متعددی دارد[35]. لیست این فایل‌ها در جدول ۳-۲ نشان داده شده است:

جدول (۳-۲) : فایل‌های پیکربندی Qmail [35]

qmail Executable Program	*Control Files*
qmail-smtpd	badmailfrom
	databytes
	localiphost
	morercpthosts
	rcpthosts
	smtpgreeting
	timeoutsmtpd
qmail-qmqpc	qmqpservers
qmail-inject	defaultdomain
	defaulthost
	idhost
	plusdomain
qmail-send	bouncefrom
	bouncehost
	concurrencylocal
	concurrencyremote
	doublebouncehost
	doublebounceto
	envnoathost
	locals
	percenthack
	queuelifetime
	virtualdomains
qmail-remote	helohost
	smtproutes
	timeoutconnect
	timeoutremote

بسته پست الکترونیکی Postfix

سیستم Postfix از پوشه‌های متعدد صف پست الکترونیکی[1] و برنامه‌های اجرایی تشکیل شده است که همگی با هم در تعامل هستند تا سرویس پست الکترونیکی را فراهم کنند[36]. شکل ۳-٤ بلوک دیاگرام هسته ای اجزای postfix را نشان می‌دهد.



شکل (۳-٤) : بلوک دیاگرام postfix

برنامه‌های اصلی postfix

Postfix از یک برنامه اصلی استفاده می‌کند که به صورت پروسه پشت زمینه، در تمام زمان‌ها در حال اجرا می‌باشد. برنامه اصلی، postfix را قادر می‌سازد تا برنامه‌هایی راه‌اندازی شوند تا صف‌های پست الکترونیکی را برای پیام‌های جدید پویش کنند و آنها را به مقصد مناسب ارسال کنند. جدول ۳-۳ برنامه‌های هسته ای را نشان می‌دهد[37].

جدول (۳-۳) : برنامه‌های هسته ای postfix

متد	توضیح
bounce	بازگشت پیام‌های بیرون انداختنی بـه فرسـتنده و پسـت در صـف پیام‌های بیرون انداختنی.
cleanup	پردازش سرآیند پست الکترونیکی‌های ورودی - پیـام‌هـا را درون صف پیام‌های ورودی قرار دادن.

[1] Mail queue

error	پردازش پیام از تحویل درخواست qmgr، اجبار پیام‌ها به بیرون انداختن.
flush	پردازش پیام‌های در حال انتظار بازیابی، برای یک سرور پست الکترونیکی راه دور است.
local	پیام‌هایی را تحویل می‌دهد که مقصدشان محلی است.
pickup	منتظر پیام‌های در صف maildrop می‌ماند و آنها را به برنامه پاکسازی می‌فرستد تا پردازش آغاز شود.
pipe	پیام‌ها را از برنامه qmgr می‌گیرد و آنها را به برنامه‌های بیرونی، ارسال می‌کند.
Postdrop	وقتی که صف، قابل نوشتن توسط کاربران عادی نیست، پیام ورودی را به صف maildrop، حرکت می‌دهد.
Qmgr	پیام‌هایی که در صف ورودی هستند را پردازش می‌کند. مشخص می‌کند که پیام‌ها چگونه و کجا باید وارد شوند و برنامه‌هایی را برای تحویل آنها، راه اندازی می‌کند.
Sendmail	ارائه رابط سازگار با sendmail توسط برنامه‌هایی برای فرستادن پیام خصوصی، به صف Maildrop.
Showq	گزارش وضعیت صف پست الکترونیکی postfix
Smtp	انتقال پیام‌ها به میزبان پست الکترونیکی بیرونی با استفاده از smtp
Smtpd	دریافت پیام‌ها از میزبان پست الکترونیکی بیرونی با استفاده از smtp
Trivial-rewrite	پیام‌ها را از برنامه cleanup دریافت می‌کند تا مطمئن شود آدرس‌های سرآیند، در فرمت استانداردی برای برنامه qmgr هستند و توسط برنامه qmgr استفاده می‌شوند تا آدرس‌های میزبان راه دور را مشخص کنند.

صف‌های پیام postfix

برخلاف دیگر بسته‌های MTA، Postfix از صف‌های متعددی برای پردازش پیام‌ها استفاده می‌کند. هر کدام از صف‌ها، مخصوص وضعیت خاصی است که برای پیام وجود دارد[37]. جدول ۳-٤ این مسئله را نشان می‌دهد.

جدول (۳-٤) : صف‌های پیام postfix

صف	توضیح
maildrop	پیام‌های جدیدی که منتظر پردازش بودند، از کاربران محلی دریافت شده‌اند.
incoming	پیام‌های جدیدی که منتظر پردازش بودند، از کاربران میزبان‌های راه دور دریافت شده‌اند. به محض اینکه کاربران محلی پردازش شوند، این اتفاق می‌افتد.
active	پیام آماده تحویل، توسط postfix می‌باشد.
deffered	پیام‌هایی که در تلاش‌های اولیه تحویل، با شکست مواجه شده‌اند، در انتظار دیگر تلاش می‌باشند.
flush	پیام مرتبط به میزبان راه دور است که به سرور پست الکترونیکی اتصال برقرار می‌کند تا بازیابی صورت گیرد.
mail	پیام‌های تحویل داده شده، ذخیره می‌شوند تا کاربران محلی آن را بخوانند.

برنامه‌های کاربردی postfix

در کنار برنامه‌های اصلی و هسته ای، postfix برنامه‌های کاربردی دیگری دارد که به مراحل پروسه پست الکترونیکی، کمک می‌کند[37]. لیست این برنامه‌ها در جدول ۳-۵ وجود دارد.

جدول (۳-۵) : برنامه‌های کاربردی postfix

برنامه	توضیح
mailq	صف پیام‌های postfix را چک می‌کند و وضعیت را نمایش می‌دهد.
postfix	شروع، خاتمه و بارگذاری سیستم postfix را کنترل می‌کند
postalias	پایگاه داده مستعار postfix را می‌سازد، بروز می‌کند و مورد پرس و جو قرار می‌دهد.
poastcat	محتوای صف‌های پیام postfix را نمایش می‌دهد.
postconf	نمایش و تغییر پارامترهای فایل پیکربندی main.cf
postkick	دستورات مورد نیاز برای اجرای postfix را ارسال می‌کند.
Postlock	فایل‌های مخصوص postfix را قفل کرده و دستورات لازم را اجرا می‌کند.
Postlog	سیستم ایجاد log در postfix می‌باشد
Postmap	یک جدول بررسی postfix را می‌سازد و مورد پرس و جو قرار می‌دهد.
Postsuper	عملیات نگهداری از یک پوشه postfix را انجام می‌دهد.

برنامه‌های پیکربندی postfix

بلوک بعدی در بلوک دیاگرام، فایل‌های پیکربندی می‌باشند. این فایل‌ها دربردارنده اطلاعاتی هستند که برنامه‌های postfix، هنگام پردازش پیام‌ها استفاده می‌کنند[37]. برخلاف بسیاری از برنامه‌های MTA، می‌توان فایل‌های پیکربندی را، حتی هنگامی که postfix در حال اجراست، تغییر داد و اثر آن را دریافت کرد.

جداول lookup در postfix

مدیر پست الکترونیکی، می‌تواند فایل‌های جدول lookup متعددی بسازد تا postfix بتواند از آنها استفاده کند. هر جدول lookup، پارامترهایی را معرفی می‌کند که تحویل پیام را کنترل می‌کند[37].

جدول (۳-٦) : postfix lookup tables

صف	توضیح
Access	میزبان‌های راه دور smtp را به یک جدول access/deny بـرای اهداف امنیتی، نگاشت می‌کند.
Aliass	گیرندگان متنوع را به صندوق پستی محلی، نگاشت می‌کند.
cannonical	اسامی صندوق پسـتی‌هـای متفرقـه را بـه صـندوق پسـتی‌هـای حقیقی، برای سرآیندهای پیام، نگاشت می‌کند.
relocated	صندوق پستی قدیمی را به صندوق پستی جدید، نگاشت می‌کند.
transport	نگاشت نام‌های دامنه را به منظور تحویل متدها، صورت می‌دهد تا اتصالات میزبان و تحویل آنها را انجام دهد.
virtual	دامنه‌هـا و گیرنـدگان، بـه صـندوق پسـتی محلـی بـرای تحویـل نگاشت می‌شوند.

مخاطرات موجود در بسته‌های پست الکترونیکی **sendmail**، **qmail** و **postfix**

پس از بررسی بسته‌های پستی sendmail، qmail و postfix، اکنون نوبت به بررسی مخاطرات این سه بسته پست الکترونیکی می‌رسد.

نداشتن مجوز مناسب فایل

داشتن مجوزهای مناسب، بخش مهمی از سیستم بسته‌های پست الکترونیکی می‌باشد. نداشتن مجوز مناسب برای فایل و پوشه‌ها، نفوذ گران را قادر خواهد ساخت که به سیستم‌تان دسترسی داشته باشند[12].

کاربری با سطح دسترسی بالا

داشتن کاربری با سطح دسترسی بالا، مانند root در این بسته‌ها، برای سیستم خطرناک می‌باشد. چون کاربر علاوه بر اینکه می‌تواند فایل‌های پیکربندی را به دلخواه خود تغییر دهد، می‌تواند به سایر قسمت‌های سیستم دسترسی پیدا کند.

در برخی بسته‌ها مانند sendmail، پیش فرض کاربر، root می‌باشد و تهدید بزرگی برای سیستم بشمار می‌رود[12].

جدول (۳-۷) : مخاطرات بسته‌های MTA

نام مخاطره	مخاطرات بسته‌های MTA
دسته حملات مرتبط با مخاطره	خواندن – دستکاری- جعل
چگونگی استفاده	نداشتن مجوز مناسب فایل و کاربری با دسترسی بالا، باعث می‌شود به فایل‌های حیاتی و اصلی سیستمی دسترسی پیدا کرده و از سیستم سوء استفاده شود.
نتیجه حملات	افشای اطلاعات- تخریب اطلاعات- دزدی خدمت- دسترسی بیشتر
حملات بعدی	–
شناسایی و محافظت	تعیین سطح دسترسی مناسب و استفاده از کاربران مناسب
سختی شناسایی	٤
آسانی استفاده	۱
فراوانی	۲
تأثیر	۵
جمع امتیاز	۳۲

۳-۲-۳ open relays

هنگامی که یک سرور پست الکترونیکی، به صورت خودکار یک پیام پست الکترونیکی را از یک کلاینت راه دور، به سرور پست الکترونیکی مقصد مناسب می‌رساند، به این مسئله رله کردن گفته می‌شود. هنگامی که یک سرور پست الکترونیکی، هر پیام را از هر کلاینت راه دور، به هر میزبان راه دور، رله می‌کند به آن سرور پست الکترونیکی Open Relay گفته می‌شود[3].

رله کردن پیام‌ها، یکی از وظایف معمول smtp می‌باشد. Smtp وسیله‌ای را برای کلاینت‌ها به وجود می‌آورد تا پیام‌هایی که مقصدشان کاربران اینترنتی است، به پست الکترونیکی سرورها بفرستند. آنها به نوبه خود می‌توانند پیام‌ها را از طریق smtp رله کنند تا به مقصد مناسب برسد. به این پروسه open relay گفته می‌شود.

رله کردن پیام‌ها توسط یک Open Relay، باعث می‌شود که هویت فرستنده از دید گیرنده پیام، پنهان شود. استفاده از این ویژگی باعث می‌شود بسیاری از بازاریابان، پیام‌های تبلیغاتی فراوانی که برای گیرنده پیام، ناخواسته است، ارسال کنند. هنگامی که قربانی آدرس پیام‌ها را نگاه می‌کند، نمی‌تواند مبدأ را رهگیری کند و این همان مورد ناخواسته ای است که open relay ایجاد کرده است.

بازاریابان انبوه[1] دنبال راهی هستند که پیام‌های تبلیغاتی خود را به mailboxهای افراد بفرستند. کلید موفقیت بازاریابی انبوه این است که تولید کننده پست الکترونیکی و مبدأ آن، ناشناخته بماند. اینجاست که open relay به این افراد کمک می‌کند پیام‌های با سرآیندهای نادرست خود را، از طریق open relay به مقصد بفرستند[3].

با افزایش پیام‌های ناخواسته تجاری، open relay بودن تبدیل به یک موضوع ناهنجار شده است. ارسال پیام‌ها از یک سرور به یک سرور دیگر، بدون هیچ درجه از گزینش، امروزه هوشمندانه نمی‌باشد. بجای آن، مقداری هوشمندی لازم است تا برای ارسال به صورت گزینشی عمل کنیم. این پروسه رله گزینشی[2] نامیده می‌شود[2]. رله گزینشی را در فصل چهارم بررسی می‌کنیم.

---

1 Mass marketer
2 Selective relaying

جدول(۳-۸) : مخاطره open relay

نام مخاطره	مخاطره Open Relay
دسته حملات مرتبط با مخاطره	سیل ریزی - جعل
چگونگی استفاده	با ارسال حجم زیاد اطلاعات، باعث از کار افتادن سرور پست الکترونیکی می‌شود.
نتیجه حملات	منع خدمت
حملات بعدی	-
شناسایی و محافظت	استفاده از رله گزینشی- بلوکه کردن پیام‌هایی که در پایگاه داده open relay جهانی، لیست شده‌اند.
سختی شناسایی	۳
آسانی استفاده	۲
فراوانی	۳
تأثیر	٤
جمع امتیاز	۳۲

۳-۲-۴ Spam

صد هزار دلار برنده شده‌اید، در ماه بیشترین حقوق را به صورت اینترنتی کسب کنید، من مردی فقیر هستم که خانواده خود را در جنگ از دست داده‌ام به من کمک کنید، عشق را

تجربه کنید و ... این‌ها عناوین پست الکترونیکی‌هایی هستند که به صورت روزانه در صندوق پستی[1] خود، مشاهده می‌کنید.

Spam، در واقع همان پیام‌های ناخواسته‌ای است که به صورت انبوه به صندوق پستی می‌رسد[38]. با افزایش spam و حجم انبوه آنها که روزانه به سرور پست الکترونیکی وارد می‌شوند، امکان از کار افتادن سرور پست الکترونیکی، وجود خواهد داشت[39]. اگر پست‌های spam مورد پردازش قرار نگیرند و حذف نشوند، سرور پست الکترونیکی با کمبود فضای روی دیسک، روبرو خواهد شد و این همان مخاطره ایست که وجود دارد. علاوه بر آن، برخی از پست‌های spam، حاوی اطلاعاتی هستند که به نفوذ گر کمک خواهد کرد با انجام عملیات مهندسی اجتماعی[2]، اطلاعات ارزشمندی همچون نام کاربری، گذر واژه[3]، حساب بانکی و دیگر اطلاعات فرد را بدست آورد یا اینکه فرد را به صفحات دلخواه خود هدایت کنند و در آنجا از کاربر سوء استفاده کنند.

روش‌هایی مانند phishing و fake page، بر اساس پست‌های spam و مهندسی اجتماعی کار می‌کنند که روش‌هایی مخرب و دارای خطر برای کاربر می‌باشند[40]. از این منظر، مدیریت و بررسی پست‌های spam، حائز اهمیت فراوانی می‌باشد. درجه اهمیت این حوزه تا حدی است که برخی در تحقیقات خود، برای موفقیت آمیز بودن جلوگیری از Spam، دولت‌ها را موظف به مدیریت و دخالت در این مسئله دانسته‌اند[21].

در فصل چهارم روش‌های جلوگیری و مقابله با پست الکترونیکی‌های spam را بررسی می‌کنیم.

---

[1] Mailbox
[2] Social engeering
[3] password

جدول(۳-۹) : مخاطره spam

نام مخاطره	مخاطره spam
دسته حملات مرتبط با مخاطره	سیل ریزی – جعل
چگونگی استفاده	با ارسال حجم زیاد اطلاعات، باعث از کار افتادن سرور پست الکترونیکی می‌شود – در پست الکترونیکی خود را فرد دیگری، معرفی کرده، سپس با راه‌های مهندسی اجتماعی از فرد سوء استفاده کرده و او را به مقصد دلخواه می‌کشاند
نتیجه حملات	منع خدمت– افشای اطلاعات
حملات بعدی	دزدی خدمت– دسترسی بیشتر
شناسایی و محافظت	بلوکه کردن پیام‌هایی که از میزبان‌های spam شناخته شده، می‌آید - بلوکه کردن پیام‌هایی که دارای subject header تجاری شناخته شده، هستند – بلوکه کردن پیام‌هایی که در پایگاه داده spam جهانی، لیست شده‌اند.
سختی شناسایی	٤
آسانی استفاده	٤
فراوانی	٥
تأثیر	٤
جمع امتیاز	٤٣

۳-۲-۵ ویروس‌ها

پست‌های spam در دنیای اینترنت، بسیار اذیت کننده می‌باشند، ولی ویروس‌ها خطرناک‌تر هستند. اثر تخریبیشان بسیاری از مدیران شبکه را مجبور کرده است تا دنبال راهی برای متوقف کردن آنها باشند.

یک ویروس یا تروجان[1] ممکن است آنچنان بلایی به سیستم وارد کند که خسارت آن جبران ناپذیر باشد[6]. خراب کردن سیستم عامل، دسترسی به سرور پست الکترونیکی، خواندن و تغییر پیام‌های سرور پست الکترونیکی، حذف کردن پست‌ها، از بین بردن اطلاعات مهم بر روی سرور، سوزاندن و از بین بردن دیسک سخت، ثبت کلیدهای زده شده[2] توسط مدیر سیستم، انتشار ویروس به دیگر سیستم‌های شبکه[20] و ... از جمله کارهایی می‌باشد که یک ویروس می‌تواند انجام داده و سرور پست الکترونیکی را به مخاطره بیندازد.

مقابله با ویروس‌ها، مهم‌ترین کاری است که مدیر سرور پست الکترونیکی بایستی انجام دهد. خطر ویروس، بسیار بیشتر از spam و open relay می‌باشد. در فصل چهارم مکانیزم‌هایی برای مقابله با ویروس ارائه می‌شود.

---

[1] trojan
[2] keylogger

جدول(۳-۱۰) : مخاطره ویروس

نام مخاطره	مخاطره ویروس
دسته حملات مرتبط با مخاطره	ترکیبی
چگونگی استفاده	با ارسال یک فایل آلوده به ویروس، تروجان یا key logger، سرور پست الکترونیکی را به نابودی بکشیم
نتیجه حملات	منع خدمت - افشای اطلاعات - تخریب اطلاعات - منع خدمت – دزدی خدمت – دسترسی بیشتر
حملات بعدی	-
شناسایی و محافظت	استفاده و نصب یک ضد ویروس قوی
سختی شناسایی	٤
آسانی استفاده	٤
فراوانی	٥
تأثیر	٥
جمع امتیاز	٤٧

۳-۳ مخاطرات سرویس پست الکترونیکی

در بخش ۳-۲ عواملی که سرور پست الکترونیکی را به مخاطره می‌اندازد، معرفی کردیم. در این قسمت به مخاطراتی که برای سرویس پست الکترونیکی وجود دارد، می‌پردازیم و در فصل چهارم راهکارهای ایمن سازی این مخاطرات را ارائه می‌دهیم.

۳-۳-۱ سوء استفاده از برخی دستورات و کاوش گری

نفوذکنندگان و spammerها، تکنیک‌های مختلفی استفاده می‌کنند تا اطلاعاتی در مورد سیستم پست الکترونیکی و کاربران آن بدست آورند. برخی از دستورات، اطلاعاتی به نفوذگر می‌دهند که می‌تواند بسیار خطرناک باشد. نمونه ای از دستورات پرمخاطره در زیر لیست شده‌اند[28].

دستور HELO: هدف دستور این است که کلاینت خودش را به سرور smtp معرفی کند. این دستور، می‌تواند مورد سوء استفاده نفوذ گران، قرار بگیرد. بدین صورت که خود را بجای فرد دیگر معرفی کنند.

دستورSEND: این دستور به منظور ارسال پیام پست الکترونیکی مستقیم، به کاربری است که از طریق ترمینال login شده است. این دستور، نقص بسیار بزرگی دارد که باعث می‌شود کاربر خارجی در هر لحظه متوجه شود چه کسی به سیستم login کرده است. نفوذ گر ها از این ویژگی استفاده می‌کنند و با گشت و گذار در اینترنت، به دنبال شناسه کاربری قربانیانی می‌گردند که به سیستم login کرده‌اند.

دستورSQML: این دستور همانند دستور send عمل می‌کند. اگر کاربر log in شده باشد، همانند send عمل می‌کند ولی اگر کاربر login نشده باشد، پیام را به mailbox گیرنده ارسال می‌کند. مخاطره ای که برای send وجود داشت، برای این دستور نیز وجود دارد.

دستورSAML: این دستور همانند دو دستور SEND و MAIL عمل می‌کند. این دستور هم به کاربر login شده، پیام می‌فرستد، هم پیام را درون mailbox کاربر، جای می‌دهد. مخاطره ای که برای send وجود داشت، برای این دستور نیز وجود دارد.

دستورVRFY: این دستور به این منظور استفاده می‌شود که پست الکترونیکی سرورهای راه دور را، برای وجود یک آدرس پست الکترونیکی، مورد پرسش قرار دهد. پست الکترونیکی سرور، در جواب ممکن است یکی از ۳ کد زیر را برگرداند:

۲۵۰: آدرس موجود است و سرور پیام‌های مربوط به آن را دریافت می‌کند

۲۵۲: آدرس ممکن است وجود داشته باشد و سرور پیام‌های مربوط به آن را دریافت می‌کند.

۵۵۰: آدرس موجود نیست و سرور پیام‌های مربوط به آن را رد می‌کند.

با ارسال مقادیر زیادی از این دستور به آدرس‌های مختلف، نفوذ گر می‌تواند آدرس‌های پست الکترونیکی را توسط کدهای برگشتی حدس بزند. علاوه بر استفاده شخصی spammer از این آدرس‌ها، برخی از نفوذ گران، این آدرس‌ها را به spammerهای دیگر می‌فروشند. یا اینکه با بدست آوردن آدرس پست الکترونیکی، نفوذ گر شروع به شکستن پسورد، برای بدست گرفتن سرور پست الکترونیکی می‌کند. در زیر نمونه ای از این کار را مشاهده می‌کنید.

$ **telnet localhost 25**

220 shadrach.ispnet1.net ESMTP sendmail 8.11.3/8.11.3; Tue, 3 Jul 2001

➥ 06:59:12 -00

EHLO shadrach.ispnet1.net

250-shadrach.ispnet1.net Hello IDENT:rich@localhost [127.0.0.1], pleased

➥ to meet you

VRFY rich

250 2.1.5 Rich Blum <rich@shadrach.ispnet1.net>

VRFY mike@shadrach.ispnet1.net

250 2.1.5 Mike Pierce <mike@shadrach.ispnet1.net>

VRFY evonne@meshach.ispnet2.net

252 2.1.5 <evonne@meshach.ispnet2.net>

VRFY alex

550 5.1.1 alex... User unknown

QUIT

221 2.0.0 shadrach.ispnet1.net closing connection

Connection closed by foreign host.

البته استثنایی هم برای این مسئله وجود دارد و آن این است که نفوذ گر هنگامی که این دستور، غیر فعال شده باشد، از RCPT TO استفاده خواهد کرد.

$ telnet localhost 25

Connected to localhost.

220 shadrach.ispnet1.net ESMTP sendmail 8.11.3/8.11.3; Tue, 3 Jul 2001

➥07:09:14 -00

EHLO shadrach.ispnet1.net

250-shadrach.ispnet1.net Hello IDENT:rich@localhost [127.0.0.1],

MAIL FROM: <badguy@otherplace.com>

250 2.1.0 <badguy@otherplace.com>... Sender ok

RCPT TO: rich

250 2.1.5 rich... Recipient ok

RCPT TO: mike@shadrach.ispnet1.net

250 2.1.5 mike... Recipient ok

RCPT TO: evonne@meshach.ispnet2.net

250 2.1.5 evonne@meshach.ispnet2.net... Recipient ok

RCPT TO: alex

550 5.1.1 alex... User unknown

QUIT

221 2.0.0 shadrach.ispnet1.net closing connection

Connection closed by foreign host.

دستور TURN: هدف این دستور، برقراری ارتباط دوطرفه بین دو کامپیوتر در انتقال پیام، توسط یک اتصال tcp می‌باشد. مشکل ایده این است که سرور smtp، به کلاینتی که خود را بجای فرد دیگری معرفی می‌کند، اعتماد می‌کند. حال اگر یک نفوذ گر به سرور smtp متصل شود و خود را بجای کامپیوتر دیگری در یک دامنه معرفی کند، تمامی پیام‌ها به سمت آن دامنه، به نفوذ گر هدایت خواهد شد.

دستور EXPN: دستور دیگری که مورد سوء استفاده قرار می‌گیرد، دستور EXPN می‌باشد. هدف این دستور این است که به میزبان راه دور اجازه دهد تا درخواست لیستی از آدرس‌های نام مستعار یا پست الکترونیکی را داشته باشد. این لیست، میزبان راه دور را قادر می‌سازد تا لیستی از پست الکترونیکی‌های واقعی داشته باشد. در لیست زیر این مسئله نشان داده شده است:

$ **telnet localhost 25**

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^]'.

220 shadrach.ispnet1.net ESMTP sendmail 8.11.3/8.11.3; Tue, 3 Jul 2001

➥ 07:19:13 -00

EHLO shadrach.ispnet1.net

250-shadrach.ispnet1.net Hello IDENT:rich@localhost [127.0.0.1],

➥ pleased to meet you

250-ENHANCEDSTATUSCODES

250-EXPN

250-VERB

250-8BITMIME

250-SIZE

250-DSN

250-ONEX

250-ETRN

250-XUSR

250 HELP

EXPN blumfamily

250-2.1.5 Rich Blum <rich@shadrach.ispnet1.net>

250-2.1.5 Barbara Blum <barbara@shadrach.ispnet1.net

250-2.1.5 Katie Jane Blum <katie@shadrach.ispnet1.net>

250 2.1.5 Jessica Blum <jessica@meshach.ispnet2.net>

EXPN postmaster

250 2.1.5 Rich Blum <rich@shadrach.ispnet1.net>

QUIT

221 2.0.0 shadrach.ispnet1.net closing connection

Connection closed by foreign host.

جدول (۳-۱۱) : مخاطره سوء استفاده از برخی دستورات و کاوش گری

نام مخاطره	مخاطره سوء استفاده از برخی دستورات و کاوش گری
دسته حملات مرتبط با مخاطره	خواندن- جعل - هدایت
چگونگی استفاده	با سوء استفاده از برخی دستورات معرفی شده، خود را جای فرد دیگری معرفی کرده و برخی شناسه‌ها را شناسایی کنیم.
نتیجه حملات	افشای اطلاعات
حملات بعدی	دزدی خدمت و تخریب اطلاعات
شناسایی و محافظت	خواندن فایل‌های log – غیر فعال کردن برخی دستورات
سختی شناسایی	۳
آسانی استفاده	۳
فراوانی	۲
تأثیر	۲
جمع امتیاز	۲۳

۳-۳-۲ سوء استفاده از سرآیند[1]های پست الکترونیکی

برخی بارها پست الکترونیکی با تأخیر بدست کاربران می‌رسد و برخی بارها پیام‌هایی می‌رسد که فرستنده آن مشخص نیست (spam).

بسته‌های spam تجاری بسیار زیادی، وجود دارد که به بازاریاب‌ها کمک می‌کند تا هزاران پست الکترونیکی جعلی، به کاربران ارسال کند.

فیلد سرآیند TO

هر دو بخش TO و FROM، قابلیت جعل دارند[41]. فیلد From به سادگی، جعل می‌شود ولی به نظر می‌رسد، اگر قسمت To جعل شود، به مقصد دلخواه نمی‌رسد، ولی این‌گونه نیست.

یکی از راه‌های جعل فیلد To، استفاده از فیلد RCPT یا Bcc در smtp می‌باشد[41]. به صورتی که وقتی درRCPT، گیرنده خود را مشخص می‌کنید، دیگر فیلد To را نادیده می‌گیرد. همچنین هنگامی که گیرنده‌ای که در RCPT مشخص شده باشد، پیغام را باز کرده و قسمت To را مشاهده می‌کند نه RCPT را. در کد smtp زیر، جعل فیلد To نشان داده شده است.

[rich@test rich]$ **telnet localhost 25**

Connected to localhost.

220 test.ispnet.net ESMTP Postfix

EHLO dude

250-test.ispnet.net

250-PIPELINING

250-SIZE 10240000

250-ETRN

250 8BITMIME

---

[1] header

MAIL FROM: <badguy@nowhere.net>

250 Ok

RCPT TO: <rich@ispnet.net>

250 Ok

DATA

From: badguy@nowhere.net

To: phonyuser@yourplace.com

Subject: This is a forged message

This is a test of a forged To: header message.

This is the end of the message test.

.

250 Ok: queued as 03792C36A

QUIT

221 Bye

Connection closed by foreign host.

[rich@test rich]$ **mail**

Mail version 8.1 6/6/93. Type ? for help.

“/var/spool/mail/rich”: 1 message 1 new

>N 1 badguy@nowhere.net Tue May 1 11:19 16/599 “This is a forged mess”

&

Message 1:

From badguy@nowhere.net Tue May 1 11:19:29 2001

Delivered-To: rich@test.ispnet.net

From: badguy@nowhere.net

To: phonyuser@yourplace.com

Subject: This is a forged message

Date: Tue, 1 May 2001 19:18:46 -0500 (EST)

This is a test of a forged To: header message.

This is the end of the message test.

&

جدول (۳-۱۲) : مخاطره سوء استفاده از سرآیندهای پست الکترونیکی

نام مخاطره	مخاطره سوء استفاده از سرآیندهای پست الکترونیکی
دسته حملات مرتبط با مخاطره	جعل - هدایت
چگونگی استفاده	با سوء استفاده از برخی سرآیندهای معرفی شده، خود را بجای فرد دیگری معرفی کرده و پست الکترونیکی Spam تولید کنیم.
نتیجه حملات	منع خدمت- افشای اطلاعات
حملات بعدی	-
شناسایی و محافظت	خواندن فایل‌های log و ردیابی
سختی شناسایی	٤
آسانی استفاده	۳
فراوانی	٤
تأثیر	۲
جمع امتیاز	۳۰

۳-۳-۳ مخاطره نا امن بودن محتوای پیام‌ها

MIME در فصل اول معرفی شد. کد گذاری که در MIME برای انتقال فایل‌های باینری ایجاد شده بود، برای پیام‌ها امنیتی ایجاد نمی‌کرد، چون با یک کدگشا[1] قابل باز شدن بود[30]. با توجه به اهمیت یک پیام، ممکن است بخواهید برای پیام، رمزنگاری استفاده کنید، اما MIME این ویژگی را نمی‌دهد. ویژگی‌های زیادی به MIME در خلال سال‌ها، افزوده شد. از جمله این ویژگی‌ها، امنیت می‌باشد که به MIME اضافه شد[43][42]. در فصل چهارم راهکارهای امن کردن MIME را بررسی می‌کنیم.

جدول (۳-۱۳) : مخاطره سوء استفاده از سرآیندهای پست الکترونیکی

نام مخاطره	مخاطره نا امن بودن محتوای پیام
دسته حملات مرتبط با مخاطره	خواندن
چگونگی استفاده	نداشتن امنیت mime، موجب می‌شود محتوای پیام‌ها لو برود.
نتیجه حملات	افشای اطلاعات
حملات بعدی	دزدی خدمت
شناسایی و محافظت	استفاده از s-mime یا pgp
سختی شناسایی	٤
آسانی استفاده	۲
فراوانی	۲
تأثیر	۳
جمع امتیاز	٢٦

[1] decoder

۳-۳-۴ نا امن بودن سرورهای POP3 و IMAP

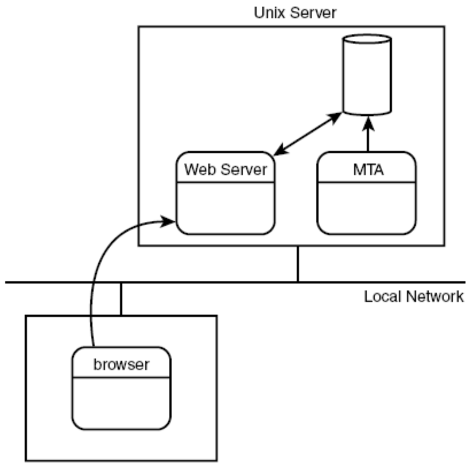
بسیاری از بسته‌های MTA برای دریافت پیام‌ها، از پروتکل‌های POP3 و IMAP بهره می‌برند. مشکل این پروتکل‌ها این است که آنها اطلاعات را به صورت متن اسکی، بدون هیچ رمزنگاری ارسال می‌کنند. اگر نفوذ گری بتواند استراق سمع کند، می‌تواند اطلاعات را به راحتی مشاهده کند. برای کمک کردن به این‌گونه مسائل، پروتکل‌های SSL و TLS به وجود آمدند که به میزبان‌های شبکه اجازه می‌دهد تا داده‌ها را قبل از ارسالشان در طول شبکه، رمز کنند[44]. این پروتکل و مسائل پیرامونی آن را در فصل چهارم بررسی می‌کنیم.

جدول (۳-۱٤) : مخاطره نا امن بودن سرورهای pop3 و imap

نام مخاطره	مخاطره ناامن بودن سرورهای imap و pop3
دسته حملات مرتبط با مخاطره	خواندن
چگونگی استفاده	فقدان رمزنگاری برای پروتکل‌های imap و pop3، باعث می‌شود تا استراق سمع صورت پذیرد.
نتیجه حملات	افشای اطلاعات
حملات بعدی	دزدی خدمت- تخریب اطلاعات
شناسایی و محافظت	استفاده از پروتکل‌های SSL و TLS
سختی شناسایی	٤
آسانی استفاده	۲
فراوانی	۳
تأثیر	٤
جمع امتیاز	۲۹

۳-۳-۵ نا امن بودن Webmail

بسیاری از شرکت‌ها، نرم افزار کلاینتی پست الکترونیکی تحت وب، منتشر کرده‌اند که کاربر را قادر می‌سازد از طریق وب، پست الکترونیکی خود را بخواند. پیاده سازی‌های بسیار زیاد و محبوبی مانند Hotmail، !Yahoo و Gmail وجود دارد که کاربران می‌توانند از طریق web browser، به سرور پست الکترونیکی متصل شوند[2]. شکل ۳-۵ این مسئله را نشان می‌دهد.



شکل (۳-۵) : استفاده از نرم افزار کلاینتی پست الکترونیکی تحت وب

بسته‌های webmail فراوانی وجود دارد که از جمله می‌توان به Squirrelmail، TWIG، Sq Webmail، IMHO، horde و roundcube اشاره کرد.

به صورت پیش فرض، قابلیت‌های امنیتی بر روی webmail وجود ندارد و بایستی قابلیت‌های امنیتی را پیکربندی کنید[45]. فقدان قابلیت‌های امنیتی برای webmail، بسیار خطرناک است. حملاتی که برای بدست آوردن گذرواژه‌webmail، اتفاق می‌افتد، حملات fake page و دیگر حملات به علت نبود امنیت در webmail به وجود می‌آید. خسارت‌های ناشی از آن می‌تواند دسترسی به پیام‌های کاربری و تغییرات در آن باشد که هزینه بسیار هنگفتی، برای کاربر دارد. امن کردن webmail، در فصل چهارم شرح داده خواهند شد.

جدول (۳-۱۵) : مخاطره نا امن بودن webmail

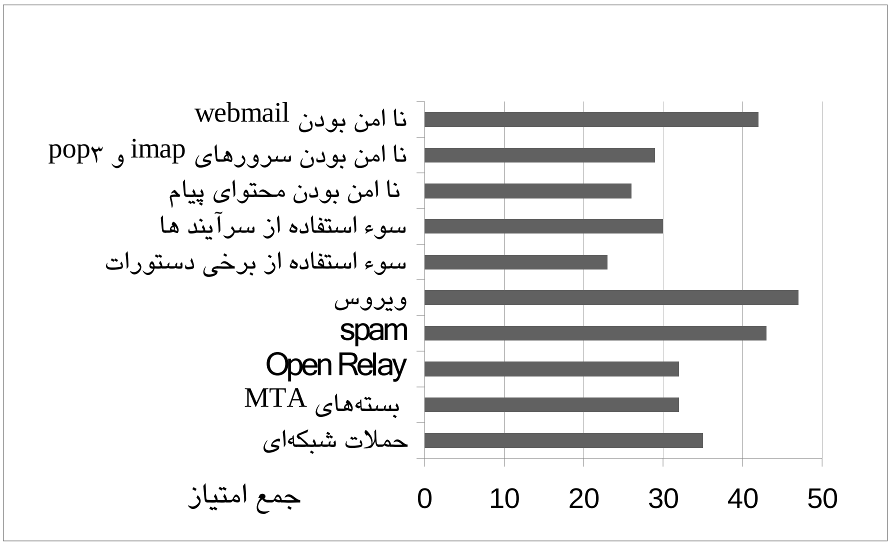
نام مخاطره	مخاطره نا امن بودن webmail
دسته حملات مرتبط با مخاطره	خواندن- دستکاری - جعل
چگونگی استفاده	فقدان رمزنگاری برای پروتکل‌های http، باعث می‌شود تا حملات خطرناکی صورت گیرد
نتیجه حملات	افشای اطلاعات
حملات بعدی	دزدی خدمت- تخریب اطلاعات
شناسایی و محافظت	استفاده از پروتکل‌های ssl و tls – امن کردن سرور apache و mysql
سختی شناسایی	٤
آسانی استفاده	۳
فراوانی	٤
تأثیر	٥
جمع امتیاز	٤۲

۳-۴ جدول و نمودار کلی

پس از ارائه جدول جزئی برای هر مخاطره، جدول کلی بر حسب درصد، برای مخاطرات ارائه می‌دهیم. در نهایت، نمودار جمع امتیاز را به صورت گرافیکی ترسیم می‌کنیم.

جدول(۳-۱۶) : جدول کلی مخاطرات

نام مخاطره	جمع امتیاز	درصد
حملات شبکه ای و دسترسی شبکه ای	۳۵	۱۰.۳
مخاطرات بسته‌های MTA	۳۲	۹.٤
مخاطره Open Relay	۳۲	۹.٤
مخاطره spam	٤۳	۱۲.٦
مخاطره ویروس	٤۷	۱۳.۸
سوء استفاده از برخی دستورات و کاوش گری	۲۳	٦.۷
سوء استفاده از سرآیندهای پست الکترونیکی	۳۰	۸.۸
مخاطره نا امن بودن محتوای پیام	۲٦	۷.٦
مخاطره نا امن بودن سرورهای imap و pop3	۲۹	۸.٥
مخاطره نا امن بودن webmail	٤۲	۱۲.۳
جمع	۳۳۹	۱۰۰



شکل(۳-٦) : نمودار کلی مخاطرات

فصل چهارم

راهکارهای ایمن سازی

این فصل، راهکارهای پیشنهادی برای رفع مخاطرات سرور و سرویس پست الکترونیکی را ارائه می‌دهد. به مباحثی همچون امن کردن سرور پست الکترونیکی، امن کردن بسته‌های پست الکترونیکی من جمله postfix، sendmail و qmail، ممانعت از open relay، بلوکه کردن spam، فیلتر کردن ویروس، رله کردن گزینشی، SASL، رمزنگاری داده‌ها توسط پروتکل‌هایی همانند SSL، TLS و PGP، استفاده از دیوارهای آتش پست الکترونیکی، امن کردن سرورهای pop3 و imap و امن کردن webmail می‌پردازیم.

برای هر راهکار و مکانیزم ارائه شده، آزمایش‌هایی صورت داده‌ایم تا متوجه شویم راهکار موجود، چقدر میزان مخاطره را کاهش می‌دهد. در واقع این آزمایش‌ها، مطالعه موردی می‌باشند و بدست آوردن مقدار دقیق این اعداد، می‌تواند موضوع تحقیقات بعدی باشد. آزمایش‌ها بر روی سرور پست الکترونیکی Qmail انجام شده است. مشخصات سیستمی که این آزمایش‌ها بر روی آن انجام شده است، به صورت زیر می‌باشد:

- CPU: 86 Family 16 Model 2 Stepping 3 AuthenticAMD ~2200 Mhz
- Qmail بر روی لینوکس CentOS 4 2.6.9-42.0.10 Elsmp نصب شده است.
- برای سیستم کلاینتی حمله کننده از Vmware و سیستم عامل Windows Xp SP3 استفاده شد.
- در هر قسمت ابزارها و پروتکل‌های مورد نیاز نصب شده‌اند.

۴-۱ ایمن سازی سرور پست الکترونیکی

در فصل سوم، مخاطراتی که برای سرور پست الکترونیکی وجود دارد، بررسی شدند. در این قسمت راهکارها و مکانیزم‌های ایمن سازی این مخاطرات را بررسی می‌کنیم.

۴-۱-۱ ایمن سازی سرورهای خانواده یونیکس[1]

مانیتورینگ فایل‌های Log

لینوکس به صورت پیش فرض، قابیلت ردیابی فعالیت‌ها را فراهم می‌کند[32]. با پیکربندی سرویس‌هایی مانند syslogd این امکان فراهم می‌شود[46]. در مثال زیر، نمونه ای از حمله را مشاهده می‌کنید که توسط سیستم log گیری وقایع، ثبت شده است و توسط مدیر شبکه قابل ردیابی می‌باشد.

May 2 16:24:49 shadrach ipop3d[5373]: port 110 service init

➥ from 192.168.1.15

May 2 16:24:49 shadrach ipop3d[5373]: Login failure user=rich

➥ host=[192.168.1.15]

May 2 16:24:52 shadrach ipop3d[5373]: AUTHENTICATE LOGIN failure

[ic:ccc host=[192.168.1.15]

May 2 16:24:52 shadrach ipop3d[5373]: Command stream end of file while

➥ readingline user=??? host=[192.168.1.15]

May 2 16:24:55 shadrach ipop3d[5374]: port 110 service init from

➥ 192.168.1.15

May 2 16:24:55 shadrach ipop3d[5374]: Login failure user=rich

➥ host=[192.168.1.15]

May 2 16:24:58 shadrach ipop3d[5374]: AUTHENTICATE LOGIN failure

➥ host=[192.168.1.15]

---

[1] unix

جلوگیری از حملات شبکه ای

قدم اول در جلوگیری از حملات شبکه ای، غیر فعال کردن هر سرویس شبکه ای است که از آن استفاده نمی‌شود. همان‌طور که در فصل مخاطرات گفته شد، ایمن سازی برنامه inetd، مهم‌ترین کار برای جلوگیری از حملات شبکه ای می‌باشد[46]. فایل /etc/inetd.conf، فایل پیکربندی inetd می‌باشد که سرویس‌ها در آن فعال شده‌اند. تمامی سرویس‌هایی که استفاده نمی‌شود، با علامت # مانند زیر غیرفعال کنید.

```
#ftp stream tcp nowait root /usr/libexec/ftpd ftpd -l
#telnet stream tcp nowait root /usr/libexec/telnetd telnetd
#shell stream tcp nowait root /usr/libexec/rshd rshd
#login stream tcp nowait root /usr/libexec/rlogind rlogind
#finger stream tcp nowait/3/10 nobody /usr/libexec/fingerd fingerd -s
#exec stream tcp nowait root /usr/libexec/rexecd rexecd
#uucpd stream tcp nowait root /usr/libexec/uucpd uucpd
#nntp stream tcp nowait usenet /usr/libexec/nntpd nntpd
#comsat dgram udp wait tty:tty /usr/libexec/comsat comsat
#ntalk dgram udp wait tty:tty /usr/libexec/ntalkd ntalkd
#tftp dgram udp wait nobody /usr/libexec/tftpd tftpd /tftpboot
#bootps dgram udp wait root /usr/libexec/bootpd bootpd
pop3 stream tcp nowait root /usr/local/libexec/popper popper -s
imap4 stream tcp nowait root /usr/local/libexec/imapd imapd
```

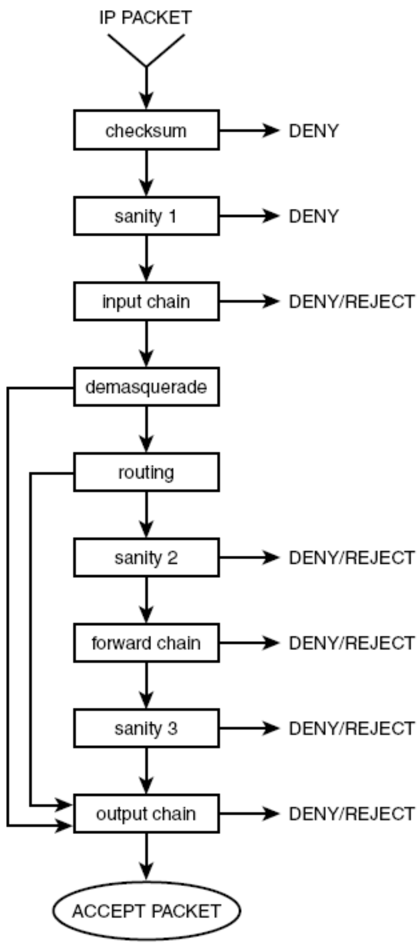
بلوکه کردن دسترسی شبکه ای به سرور

با راه اندازی دیوار آتش، بر روی سرور، این امکان به وجود می‌آید که ترافیک‌ها دسته بندی شوند و آنها را در صورت لزوم بلوکه کنید. با راه اندازی iptables و ipchanis در لینوکس، این قابلیت را پیدا خواهید کرد[47].

Ipchains پروسه‌هایی دارد که در جدول ٤-١ و شکل ٤-١ مشخص شده اند.

جدول (٤-١) : پروسه‌های ipchain در فیلتر کردن بسته‌ها

صف	توضیح
checksum	بسته‌های خراب شده را بررسی می‌کند
Sanity1	بسته‌های تغییر یافته را بررسی می‌کند
Input chain	بررسی زنجیره ورودی فایروال
demasquerade	اگر بسته ای نقاب زده شده باشد، آن را به بسته اصلی تبدیل کند.
routing	اگر بسته نیاز باشد که به جلو هدایت شود، مقصد بررسی شود.
Sanity2	بسته‌های تغییر یافته را بررسی می‌کند
Forward chain	بررسی زنجیره هدایت فایروال
Sanity2	بسته‌های تغییر یافته را بررسی می‌کند
output chain	بررسی زنجیره خروجی فایروال



شکل (۴-۱) : پروسه های ipchain در فیلتر کردن بسته ها

استفاده کردن از سیستم‌های IDS[1] یا IPS[2]

اگرچه با راه اندازی فایروال، روی سرور می‌توانید سدی مقابل حملات شبکه به وجود آورید، اما این کافی نیست. اگر به سرور، به هر نحوی دسترسی پیدا شود و درب پشتی بر روی سیستم نصب شود، می‌تواند بسیار خطرناک باشد. در اینجا توصیه می‌شود که ipsهایی مانند tripwire، بر روی سرور نصب شوند[48].

[1] Intrusion Detection System
[2] Intrusion Prevention System

محاسبه میزان کاهش مخاطره

برای تست کاهش مخاطره چند کار صورت گرفت:

- سرویس‌های اضافی inetd، غیر فعال شدند.
- در iptables قواعد مناسبی نوشته شد و جلوی دسترسی‌های اضافی گرفته شد. این قواعد در زیر لیست شده‌اند.

```
ipchains -P forward DENY/sbin/ipchains -A forward -i  ppp0 -j MASQ
ipchains -A input -I ppp0 --destination-port smtp -y -j ACCEPT
ipchains -A input -i ppp0 -l -y -j DENY
```

- جلوی تمام دسترسی‌ها بجز smtp گرفته شد.
- فایل‌های log در هر حمله بررسی شدند و به ازای حملات در iptables و ipchains، یک قاعده اضافه شد.
- حملات با ipهای مختلفی انجام شد.
- حملات برای ۱۰۰۰ نمونه اجرا شد.

برای تست، سعی شده است به سرویس‌های مختلف، اتصال ایجاد شود، اما چون هم در inetd سرویس‌ها غیر فعال بودند، هم در iptables و ipchains جلوی آن‌ها گرفته می‌شد، deny رخ می‌داد و حمله صورت نمی‌گرفت.

Unable to connect to remote host: Connection refused

نتیجه آزمایش بدین صورت بود که با اعمال موارد فوق، از ۱۰۰۰ حمله، هیچ حمله‌ای موفقیت آمیز نبود. یعنی جمع امتیاز مخاطره پس از این کار، به صفر رسید.

جدول (٤-٢) :میزان کاهش مخاطره حملات شبکه ای و دسترسی شبکه ای

نام مخاطره	حملات شبکه ای و دسترسی شبکه ای
شناسایی و محافظت	ایمن سازی inetd – نصب فایروال و IPS و IDS
تعداد آزمایش‌های صورت گرفته	۱۰۰۰
تعداد حملات موفق	۰
تعداد حملات نا موفق	۱۰۰۰
جمع امتیاز قبل از ایمن سازی	۳۵
میزان کاهش مخاطره(درصد)	۱۰۰
جمع امتیاز پس از ایمن سازی	۰

۴-۱-۲ ایمن سازی بسته پست الکترونیکی Sendmail

در سال‌های پیش، مدیران سرور پست الکترونیکی، ویژگی‌هایی را فعال می‌کردند تا sendmail امن گردد، ولی امروزه این ویژگی‌ها به صورت پیش فرض در sendmail فعال هستند و لازم نیست چیزی تغییر داده شود[33]. در اینجا این ویژگی‌ها را معرفی کرده و بررسی می‌کنیم که چگونه این ویژگی‌ها، sendmail را امن می‌سازد.

مجوزهای فایل

Sendmail مجوزها و سیاست‌های مالکیتی سفت و سختی بر روی سیستم سرور پست الکترونیکی، در نظر گرفته است. اگر سیاست‌های امنیتی نقض شوند، sendmail پیام‌های هشدار ارسال می‌کند. اکنون بسیاری از محدودیت‌ها بر روی فایل‌ها و دایرکتوری‌ها، توسط sendmail اعمال شده است[49]. اکثر آنها به دو دسته کلی تقسیم می‌شوند:

- Sendmail فایل‌هایی که مجوز نوشتن دارند را نمی‌خواند، نمی‌نویسد و اجرا نمی‌کند.
- Sendmail فایل‌های درون پوشه‌هایی که مجوز نوشتن دارند را نمی‌خواند، نمی‌نویسد و اجرا نمی‌کند.

به عنوان مثال، فایل sendmail.cf یا پوشه /etc/mail که دارای مجوزهای نوشتن هستند را نمی‌خواند و یک پیام هشدار، صادر می‌کند.

/etc/mail/sendmail.cf: WARNING: dangerous write permissions

کاربران sendmail

Sendmail سه دسته کاربر زیر را تعریف کرده است[49]:

TrustedUser

DefaultUser

RunAsUser

همان‌گونه که در فصل سوم ذکر شد، به صورت پیش فرض، sendmail کاربر root را به عنوان کسی در نظر می‌گیرد که می‌تواند sendmail را اجرا کند و فایل‌های پیکربندی آن را دست‌خوش تغییر قرار دهد. این پیش فرض بایستی تغییر کند.

گزینه TrustedUser: با این گزینه می‌توانید کاربر یا کاربرانی را تعریف کنید که sendmail به آنها اجازه می‌دهد مالک فایل‌هایی شوند که توسط sendmail، مورد دسترسی قرار می‌گیرد. با این گزینه می‌توانید مدیران پست الکترونیکی تعریف کنید که مسئول نگهداری جداول sendmail باشند، بدون اینکه مجوزهای root را به فرد بدهید.

گزینه DefaultUser: با این گزینه می‌توانید به sendmail اجازه دهید که برنامه‌های نامه رسان مجزایی، مانند procmail تحت قالب این گزینه، بجای کاربر root، برنامه را اجرا کند[50]. به صورت پیش فرض، sendmail برنامه‌های نامه رسان را به وسیله کاربری به نام mailnul اجرا می‌کند. تنها در صورتی که این کاربر را پیدا نکند، سراغ کاربر root می‌رود.

گزینه RunAsUser: با این گزینه می‌توانید کاربر یا کاربرانی تعریف کنید که sendmail، با مجوز آنها بعد از شروع، عمل می‌کند. با محدود کردن مناطقی که کاربر می‌تواند فعالیت کند،

جلوی دسترسی به فایل‌های مهم را توسط نفوذ گر می‌گیرید. در زیر مجوزهای RunAsUser مشخص شده است :

• Write access to the /var/spool/mqueue directory

• Write access to the /var/log/maillog file

• Read access to the sendmail.cf file and any other sendmail tables used

۴-۱-۳ Qmail و امنیت

پیکربندی پیش فرض qmail، ویژگی‌های امنیتی و قابلیت اطمینان بسیار زیادی را پشتیبانی می‌کند[35][34]:

- برای اجرای برنامه‌های qmail، از شناسه‌های کاربری متعدد و متفاوتی استفاده می‌شود.
- Qmail استفاده از کاربر root را بسیار محدود می‌کند.
- پیام‌ها فوراً درون صف‌های پیام دو بخشی ذخیره می‌شوند تا از شلوغی پوشه‌ها و پیام‌های گم شده، به خاطر نقص سیستم جلوگیری شود.
- Qmail سیستم بسیار دقیق و همراه با جزئیات Logging دارد.

تمامی این ویژگی‌ها به صورت پیش فرض در qmail وجود دارد و نیاز به انجام تنظیمات اضافی وجود ندارد.

محاسبه میزان کاهش مخاطره

همان‌طور که ذکر شد، Qmail به صورت پیش فرض، ویژگی‌های امنیتی بسیاری را فعال کرده است و باعث شده است که بسیاری از افراد، Qmail را یک MTA امنیتی قوی بشناسند. در اینجا با اینکه Qmail، استفاده از کاربر root را محدود کرده است ولی هنوز از آن استفاده می‌کند و این یک مخاطره محسوب می‌شود. البته نفوذ به سیستم، بسیار دشوار است و از هزار نفر، ممکن است فقط تعداد انگشت شماری بتوانند از کاربر root سوء استفاده کنند. در آزمایش، امکان دسترسی از طریق qmail به کاربر root به وجود نیامد ولی احتمال دسترسی توسط نفوذ گران حرفه ای که در دنیا کم شمار هستند، وجود دارد.

در آزمایش‌های صورت گرفته، فایل‌ها و برنامه‌های qmail بررسی شدند تا رخنه ای پیدا شود ولی نتیجه ای حاصل نشد.

جدول (٤-٣) : میزان کاهش مخاطرات بسته‌های MTA (Qmail)

نام مخاطره	مخاطرات بسته‌های MTA (Qmail)
شناسایی و محافظت	ویژگی‌های امنیتی بسیاری به صورت پیش فرض، فعال هستند: - برای اجرای برنامه‌های qmail از شناسه‌های کاربری متعدد و متفاوتی استفاده می‌شود. - Qmail استفاده از کاربر root را بسیار محدود می‌کند. ...
کیفیت آزمایش‌های صورت گرفته	فایل‌ها و برنامه‌های qmail بررسی شدند تا رخنه ای یافت شود.
تعداد حملات موفق	۰
حملات نا موفق	هیچ فایل و برنامه ای، حاوی رخنه تشخیص داده نشد.
جمع امتیاز قبل از ایمن سازی	۳۲
میزان کاهش مخاطره(درصد)	۱۰۰
جمع امتیاز پس از ایمن سازی	۰

۴-۱-۴ postfix و امنیت

به صورت پیش فرض، postfix ویژگی‌های امنیتی بسیار زیادی دارد. علاوه بر قابلیت‌های امنیتی qmail، postfix دو قابلیت امنیتی اضافه دارد که هنگام نصب postfix، به صورت پیش فرض می‌توانید آنها را فعال کنید[37][36].

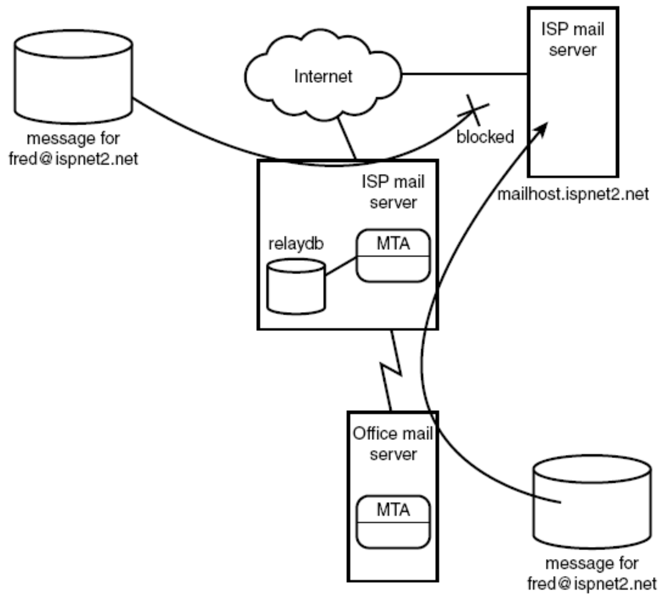
- مشخص کردن امنیت maildrop در postfix: به عنوان مدیر پست الکترونیکی می‌توانید میزان امنیت را مشخص کنید. به صورت پیش فرض، پوشه صف پیام‌های maildrop، توسط تمام کاربران محلی قابل نوشتن است. این مسئله کاربران محلی را قادر می‌سازد تا خودشان به صورت دستی بتوانند در این صف، ورودی ایجاد کنند. اگر با این مسئله مشکل داشته باشید می‌توان کاری کرد که فقط افراد و گروه‌های خاصی، دسترسی داشته باشند.

- نصب کردن postfix در محیط chroot: یک مسئله امنیتی بسیار مهم این است که postfix، تنها از یک منطقه محدود شده درون سرور پست الکترونیکی، قابل اجرا باشد. این ویژگی باعث می‌شود که اگر نفوذی به سیستم پست الکترونیکی به وجود آید، تنها به همان منطقه، محدود شده باشد و نفوذ گر به دیگر فایل‌های سیستمی و سیستم، دسترسی نداشته باشد. این کار توسط برنامه chroot قابل انجام است.

۵-۱-۴ اجتناب از open relay

Open relay هنگامی اتفاق می‌افتد که یک سرور پست الکترونیکی، تلاش می‌کند یک پست الکترونیکی که مرتبط به پست الکترونیکی سرور دیگر است، به پست الکترونیکی سرورتان بفرستد، سرورتان پیام را می‌پذیرد و آن را به پست الکترونیکی سرور دیگر می‌فرستد. اما سوء استفاده از این مسئله موجب شده است که تمهیداتی در نظر گرفته شود تا جلوی open realy گرفته شود[3].

اگر رله را روی پست الکترونیکی سرور غیر فعال کنید، هیچ یک از مشتریان قادر نخواهد بود پیامش را به کاربران دیگر سرورهای پست الکترونیکی و کاربران اینترنتی بفرستد. گزینه بهتر، همان رله گزینشی می‌باشد[12]. شکل ٤-٢ این مسئله را نشان می‌دهد.



شکل (۴-۲) : selective relying

پیکربندی رله گزینشی[1]

بسیاری از بسته‌های MTA امروزی، به صورت پیش فرض از open relay بودن ممانعت می‌کنند. بهر حال اگر خواستار رله گزینشی باشید، بایستی به صورت مشخص و اختصاصی آن را پیکر بندی کنید.

پیکربندی رله گزینشی در Sendmail

نسخه‌های اولیه sendmail، از open relay بودن ممانعت به عمل نمی‌آوردند، اما در نسخه‌های جدید و امروزی، از open relay ممانعت به عمل می‌آید. برای پیکربندی رله گزینشی، بایستی جداول دسترسی تعریف کنید[2]. فرمت جدول دسترسی به صورت دو ستونه می‌باشد که در ستون اول، میزبان و در ستون دوم، عملی که باید صورت گیرد را مشخص می‌کند(host action). ۵ حالت برای action داریم که در زیر لیست شده‌اند.

OK: میزبان راه دور می‌تواند پیام را به سمت سرور پست الکترونیکی بفرستد.

---

[1] Selective relaying

RELAY: میزبان راه دور می‌تواند پیام را از طریق پست الکترونیکی سرور، به پست الکترونیکی سرورهای راه دور دیگر، رله کند.

REJECT: میزبان راه دور، اجازه ندارد پیام را به سمت پست الکترونیکی سرور و یا از طریق پست الکترونیکی سرور بفرستد.

DISCARD: پیام‌های رسیده از طریق میزبان راه دور، دور انداخته می‌شود و هیچ پیغامی به میزبان، نمایش داده نمی‌شود.

Nnn text: پیام‌های رسیده از طریق میزبان راه دور، دور انداخته می‌شود و پیغامی به میزبان، نمایش داده می‌شود.

در زیر، نمونه ای از جدول دسترسی را مشاهده می‌کنید

192.168. RELAY

ispnet1.net OK

spammer.net REJECT

mail1.anotherspammer.com REJECT

badguy.net 550 Sorry, we don’t allow spammers here

nuisance.trouble.com DISCARD

توسط دستورات زیر، این جدول را به فایل پیکر بندیsendmail، تخصیص می‌دهید:

Kaccess hash /etc/mail/access

makemap /etc/mail/access < /etc/mail/access.txt

پیکربندی رله گزینشی در Qmail

به صورت پیش فرض، qmail تنها در صورتی به عنوان open relay کار می‌کند که فایل پیکربندی rcpthosts، موجود نباشد. در یک نصب معمولی، قرار دادن محتویات فایل پیکربندی me بجای rcpthosts، موجب می‌شود که از open relay بودن ممانعت به عمل آید. فایل rcpthosts، آدرس‌هایی که qmail-smtpd می‌تواند بپذیرد را کنترل می‌کند. اگر میزبان راه دور، پیامی را به آدرسی که در فایل rcpthosts موجود نباشد، بفرستد qmail-smtpd آن را نمی‌پذیرد و رد می‌کند[2].

یک استثنا برای این مسئله وجود دارد و آن اینست که اگر متغیرRELAYCLIENT، مقدار داشته باشد، فایل rcpthosts نادیده گرفته خواهد شد و تمام پیام‌ها به سمت آدرس‌های راه دور مشخص شده در RELAYCLIENT، هدایت می‌شوند. در زیر، دو روش برای مقدار دهی متغیر محیطی RELAYCLIENT و پیاده سازی رله گزینشی شرح داده شده است.

استفاده از برنامه tcpwrapper

برنامه tcpwrapper یک برنامه یونیکسی رایج است که به عنوان مرد میانی[1] همراه با برنامه inetd، مورد استفاده قرار می‌گیرد[51]. این برنامه ویژگی‌های دیگری برای inetd ایجاد می‌کند که در زیر لیست شده‌اند.

- پایگاه داده ای از آدرس‌های ip، برای اجازه دادن و اجازه ندادن ایجاد می‌کند.
- سیستم logging، افزوده ای برای اتصالات، ایجاد می‌کند.
- اسم کامپیوتر و ip آن را از طریق dns، بررسی می‌کند.
- اگر از inetd برای مانیتورینگ شبکه برای اتصالات smtp استفاده می‌کنید، می‌توانید از tcpwrapper استفاده کنید تا به smtp قابلیت رله گزینشی بدهید.

پیکربندی tcpwrapper

برای پیاده سازی رله گزینشی توسط tcpwrapper، بایستی پایگاه داده کنترل دسترسی را برای tcpwrapper ایجاد کنید[12]. فرمت کلی به صورت زیر است:

daemon_list : client_list [: shell_command]

daemon_list برنامه ای را مشخص می‌کند که قانون دسترسی بایستی با آن منطبق شود.

Client_list آدرسی را مشخص می‌کند که قانون دسترسی بایستی با آن منطبق شود.

Shell_command دستور پوسته[2] را مشخص می‌کند که متغیرRELAYCLIENT را مقدار دهی می‌کند تا تابع رله qmail-smtpd راه اندازی شود.

پایگاه کنترل دسترسی، درون فایلی بنام host.allow قرار دارد. نمونه ای از محتویات این فایل را در زیر مشاهده می‌کنید.

tcp-env: 192.168.: setenv = RELAYCLIENT

---

[1] Man in the middle
[2] shell

tcp-env: localhost: setenv = RELAYCLIENT

خط اول، کل آدرس ۱۹۲.۱٦۸.۰.۰ را و خط دوم، خود میزبان را نشان می‌دهد.

خط زیر را هم باید در inetd.conf اضافه کنید تا از tcpwrapper استفاده شود.

/var/qmail/bin/tcp-env /var/qmail/bin/qmail-smtpd

استفاده از برنامه tcpserver

می‌توانید بجای inetd، از tcpserver نیز بهره بگیرید. Tcpserver ویژگی‌های بیشتری مانند ویژگی‌های زیر، نسبت به inetd دارد[32].

- می‌تواند تمامی ورودی و خروجی‌ها را درون یک فایل، ثبت کند.
- می‌تواند ویژگی‌های کنترل دسترسی برای اجازه اتصال یا عدم آن را، از کلاینت‌های گزینش شده، ایجاد کند.
- دارنده محدودیت‌های همزمانی، برای جلوگیری از سر بارگذاری سیستم می‌باشد.

پیکربندی tcpserver

برنامه tcpserver همانند برنامه tcpwrapper دارای پایگاه داده کنترل دسترسی است[12]. فرمت این پایگاه داده به صورت زیر است:

address:action

نمونه این پیکربندی در زیر آمده است :

192.168.:allow,RELAYCLIENT=""

192.168.1.10:deny

در خط اول، relaying برای آدرس 192.168.0.0 فعال شده است و برای ۱۹۲.۱٦۸.۱.۱۰ غیرفعال شده است. (وقتی RELAYCLIENT خالی باشد، relay فعال می‌شود).

اجتناب کردن از open relayها

نه تنها، نبودن سرور open relay مهم است، بلکه نپذیرفتن پیام‌ها از سرورهای open relay مشهور نیز، حائز اهمیت است[52].

سیستم‌های متعددی وجود دارد که لیست سیاهی[1] از سایت‌های open relay، ارائه می‌دهند[12]. برخی از این سیستم‌ها در زیر لیست شده‌اند:

Open Relay Blacklist System (ORBS)

MAPS Realtime Blackhole List (RBL)

می‌توانید این سایت‌ها را در MTA پیکربندی کنید.

محاسبه میزان کاهش مخاطره

برای تست کاهش مخاطره چند کار صورت گرفت:

- مهم‌ترین کار در این آزمایش این است که پیام‌ها را از سرورهای open relay مشهور نپذیرید.

```
vi /var/qmail/control/blacklists
-r zen.spamhaus.org -r list.dsbl.org -r combined.njabl.org
vi /etc/tcprules.d/tcp.smtp
```

- در وهله دوم، بایستی خودش Open Relay نباشد. با توجه به رله گزینشی، مشخص می‌کنیم که پیام‌ها را به کدام سرورها رله کند.

```
192.168.:allow,RELAYCLIENT="",DKSIGN="/var/qmail/control/domaink
eys/%/private",RBLSMTPD="",NOP0FCHECK="1",
DKVERIFY="DEGIJKfh",DKQUEUE="/var/qmail/bin/qmail-
queue.orig",GREY=""
```

گلوگاه[2] در open relay، همان مسئله اول می‌باشد. یعنی پیام‌ها را از سوی سرورهای open relay مشهور نپذیرد[12]. ممکن است سروری open relay باشد ولی در این لیست نیامده باشد. با توجه به اینکه open relay شدن و ثبت شدن در این لیست‌های جهانی، کار آسانی نیست، احتمال موفقیت آمیز بودن مخاطره open relay با مکانیزم‌های بکار گرفته، وجود دارد ولی بسیار کم است. در آزمایشی که صورت گرفت، از دو سرور پست الکترونیکی qmail بر روی vmware استفاده شد و در لیست داده شده برای تست، ۸۰ دامنه لیست شده

[1] Blacklist
[2] Bottleneck

در RBLها و ۲۰ دامنه خارج از آنها داده شد. نتیجه این بود که ۸۰ دامنه لیست شده در RBL، بلوکه شدند ولی ۲۰ دامنه بلوک نشده و حمله به آنها، موفقیت آمیز بود. البته این اعداد، قابل تغییر می‌باشند چون ممکن است گفته شود تعداد دامنه‌هایی که در لیست‌های RBL نیستند، نسبت به آن‌هایی که وجود دارند، بسیار کم‌تر است. در زیر نمونه ای از خروجی حمله مشاهده می‌شود.

```
# DNS based IP address spam list blackholes.mail-abuse.org

R$* $: $&{client_addr}

R::ffff:$-.$-.$-.$- $: <?> $(host $4.$3.$2.$1.blackholes.mail-abuse.org. $:

➥ OK $)

R$-.$-.$-.$- $: <?> $(host $4.$3.$2.$1.blackholes.mail-abuse.org. $:

➥ OK $)

R<?>OK $: OKSOFAR

R<?>$+ $#error $@ 5.7.1 $: "550 Mail from " $&{client_addr} " refused

➥ by blackhole site blackholes.mail-abuse.org"
```

جدول (٤-٤) : میزان کاهش مخاطره open relay

نام مخاطره	مخاطره Open Relay
شناسایی و محافظت	پیام‌ها را از سرورهای open relay مشهور نپذیرید- با توجه به رله گزینشی، مشخص می‌کنیم که پیام‌ها را به کدام سرورها، رله کند.
تعداد آزمایش‌های صورت گرفته	۱۰۰
تعداد حملات موفق	۲۰
حملات نا موفق	۸۰
جمع امتیاز قبل از ایمن سازی	۳۲
میزان کاهش مخاطره(درصد)	۸۰
جمع امتیاز پس از ایمن سازی	٦.٤

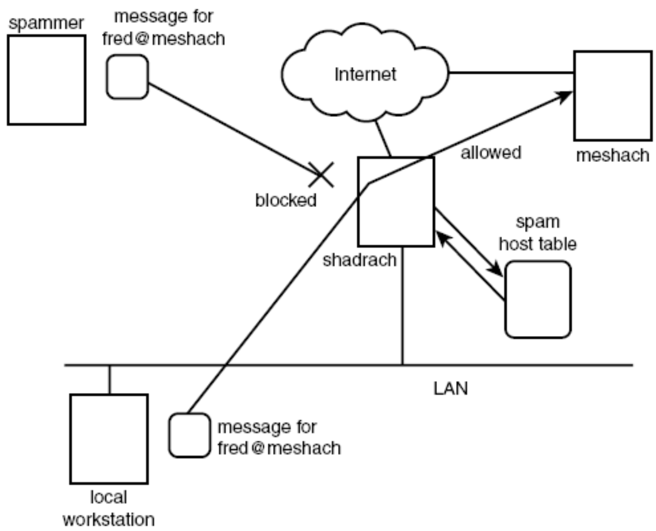
۴-۱-۶ بلوکه کردن Spamها

از ابتدای به وجود آمدن اینترنت، متدهای زیادی برای جلوگیری از spam معرفی شده است[53]. ۳ متد کلی برای بلوک کردن spamها، تا به حال معرفی شده است[2].

- ممانعت کردن از قبول پیام‌ها، از میزبان‌های spam مشهور.
- اعتبارسنجی اطلاعات جلسه smtp که با میزبان راه دور، تهیه شده است
- فیلتر کردن پیام‌های ورودی، به منظور جستجو برای علائم وجود spam

ممانعت کردن از قبول پیام‌ها از میزبان‌های spam مشهور

همانند open relay، می‌توانید با داشتن لیستی از میزبان‌های spam مشهور، از قبول پیام‌های آنها خودداری کنید[2]. شکل ٤-۳ این مسئله را نشان می‌دهد.



شکل (٤-٣) : بلوک کردن پیام‌های دریافتی از میزبان‌های spam مشهور

برای پیاده سازی دو متد داریم :

– لیست خودتان را از میزبان‌های spam بسازید تا سرور پست الکترونیکی، آن را چک کند.

– به سرورهای اینترنتی که لیست میزبان‌های spam مشهور را ارائه می‌دهند، متصل شوید.

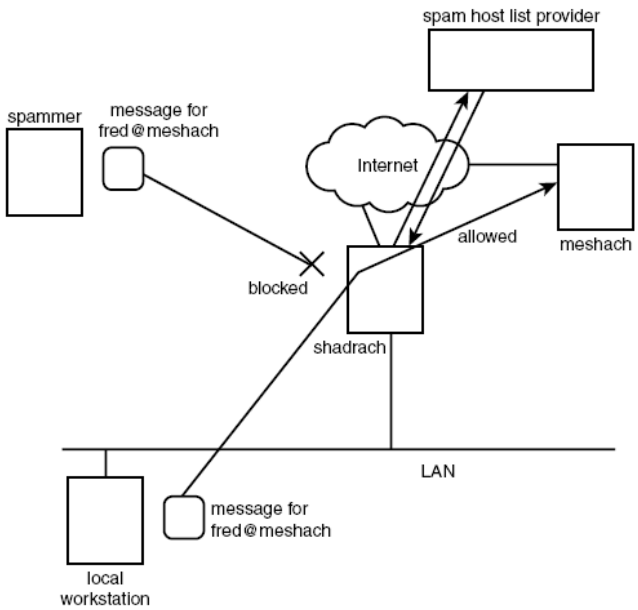
ایجاد لیست خودتان از میزبان‌های spam

در این متد، باید اطلاعات را درون یک lookup table وارد کنید[2]. چون بسیاری ازspammerها، اطلاعات تقلبی به عنوان آدرس بازگشت وارد می‌کنند، بایستی مراقب باشید. برای جلوگیری از این مسئله می‌توانید بجای آدرس پست الکترونیکی یا نام کاربری، آدرس میزبان را در لیست وارد کنید. این متد موثر است اما باید مراقب باشید که این کار می‌تواند کاربران زیادی از یک میزبان را بلوکه کند. نقطه ضعف این روش این است که نمی‌توانید میزبان‌های spam را شناسایی کنید، مگر اینکه از طرف آنها به کاربرتان، پستی ارسال شود. شناسایی spammerهای جدید، کار دشواری است. البته می‌توانید به سایت‌هایی مانند www.spamcop.net که این لیست را ارائه می‌دهند، مراجعه کنید و تک تک آدرس‌ها را استخراج و آنها را در لیست محلی خودتان، ثبت کنید.

استفاده از ارائه دهنده لیست میزبان‌های spam

همانند آنچه برای open relay ذکر شد، برخی سایت‌ها و سرورها، لیستی از میزبان‌های spam مشهور را ارائه می‌دهند[2]. می‌توانید با اتصال به آنها، از spam ممانعت به عمل آورید. شکل ٤-٤ این مسئله را نشان می‌دهد.

MAPS همان‌گونه که لیستی از open relayها را داشت، لیستی از spamها را نیز دارد و در این امر می‌تواند کمک کند.



شکل (٤-٤) : استفاده از یک سرور اینترنتی برای شناسایی میزبان‌های spam مشهور

اعتبار سنجی اطلاعات جلسه smtp

همان‌طور که قبلاً بحث شد، spammerها می‌توانند اطلاعات جعلی از هویت، مانند آدرس فرستنده، برای گیرنده پیام بفرستند. بسیاری از MTAها قابلیت چک کردن اطلاعات را می‌دهند[2]. دو متدی که برای این کار استفاده می‌شود: HELO و MAIL FROM.

دستور HELO که بایستی در مقابل آن، اسم میزبان ذکر شود، اکثراً توسط spammerها مورد سوء استفاده قرار می‌گیرد و اطلاعات جعلی در آن وارد می‌شود. توسط برخی از بسته‌های MTA، می‌توان برای جلوگیری از تقلب، اقدام به سؤال جستجوی DNS برای

تطابق اسم و ip کرد و بدین صورت، فرستنده پیام را مجبور کنیم تا اطلاعات دقیق و درست وارد کند.

قسمت MAIL FROM که آدرس فرستنده را مشخص می‌کند، نیز همانند HELO می‌توان برای جلوگیری از تقلب، اقدام به سؤال جستجوی DNS، برای تطابق اسم و ip کرد و بدین صورت، فرستنده پیام را مجبور کنیم تا اطلاعات دقیق و درست وارد کند.

فیلتر کردن پست الکترونیکی‌های spam

آخرین متد بلوکه کردن spam، استفاده از قابلیت‌های فیلترینگ بر روی بسته MTA می‌باشد که برای جستجوی عبارت موجود درون پست‌های spam، استفاده می‌شود[2]. اگر عبارت خاصی که معمولاً در پست‌های spam وجود دارد، در پیام وجود داشته باشد، آن پیام پذیرفته نخواهد شد. جستجوی پیام می‌تواند شامل دو قسمت باشد: سرآیند[1] پیام و بدنه[2] پیام.

پیاده سازی بلوکه کردن spam روی Qmail

Qmail به صورت پیش فرض جلوی spamها را می‌گیرد. همچنین برنامه‌های افزودنی qmail نیز وجود دارند که این کار را می‌کنند.

ایجاد لیست خودتان از میزبان‌های spam

فایل کنترلی badmailfrom به منظور ایجاد لیستی از آدرس‌های پست الکترونیکی که سرور qmail از گرفتن پست الکترونیکی از آنها معذور است، استفاده می‌شود[34]. مانند زیر:

nuisance@advert.corp1.com

@mail.hq.corp.com

@evildomain.net

$ **telnet localhost 25**

Connected to localhost.ispnet1.net.

220 shadrach.ispnet1.net ESMTP

---

[1] header
[2] body

HELO evildomain.net

250 shadrach.ispnet1.net

MAIL FROM: <badguy@evildomain.net>

250 ok

RCPT TO: <rich@ispnet1.net>

553 sorry, your envelope sender is in my badmailfrom list (#5.7.1)

QUIT

Connection closed by foreign host.

استفاده از سرور MAPS RSS

برنامه qmail می‌تواند اتصالات ورودی را با سرور MAPS RSS، توسط برنامه rblsmtpd، چک کند[35].این حالت، دقیقاً مشابه حالتی است که در مورد open relay بکار رفت. دستور این کار به صورت زیر است:

/usr/local/bin/tcpserver -v -R -H -l 0 -x /etc/tcp.smtp.cdb -c "$MAXSMTPD"

➥ -u $QMAILDUID -g $NOFILESGID 0 smtp /var/qmail/bin/rblsmtpd

➥ -r "blackholes.mail-abuse.org: Your

➥ site has been listed in the MAPS RSS database"

➥ /var/qmail/bin/qmail-smtpd

استفاده از فیلتر کردن پیام‌ها

Qmail اولیه، این قابلیت را پشتیبانی نمی‌کرد ولی پس از گذشت زمان، برنامه‌ها و بسته‌های افزودنی بسیار زیادی برای qmail نوشته شد. یکی از محبوب‌ترین این بسته‌ها qmail-qfilter می‌باشد[35][34]. این برنامه به زبان perl می‌باشد و پیام را قبل از وارد شدن به صف، فیلتر می‌کند. نمونه ای از این فیلتر، بر اساس موضوع و فرستنده، در زیر آورده شده است:

```
while(<>) {
print;
exit 31 if /^Subject: Make more money/;
exit 31 if /^Subject: An important offer from/;
exit 31 if /^Subject: From your friends at/;
exit 31 if /^Subject: How to be a millionaire/;
exit 31 if /^From: 1234\@spamco.com/;
}
```

```
#!/bin/sh
exec /var/qmail/bin/qmail-qfilter /var/qmail/bin/deny-spam
```

```
$ telnet localhost 25
Connected to localhost.
EHLO spamco.com
250-shadrach.ispnet1.net
250-PIPELINING
250 8BITMIME
MAIL FROM: 1234@spamco.com
250 ok
RCPT TO: rich@shadrach.ispnet1.net
250 ok
DATA
354 go ahead
```

From: 1234@spamco.com

To: rich@shadrach.ispnet1.net

Subject: Sample spam session

This session should be blocked by our spam script!

.

554 mail server permanently rejected message (#5.3.0)

QUIT

221 shadrach.ispnet1.net

Connection closed by foreign host.

محاسبه میزان کاهش مخاطره

برای تست کاهش مخاطره چند کار صورت گرفت:

- همانند open relay، مهم‌ترین کار در این آزمایش این است که پیام‌ها را از سرورهای spam مشهور نپذیرید.

smtpd_client_restrictions = reject_maps_rbl

maps_rbl_domains = blackholes.mail-abuse.org

/usr/local/bin/tcpserver -v -R -H -l 0 -x /etc/tcp.smtp.cdb -c "$MAXSMTPD"

-u $QMAILDUID -g $NOFILESGID 0 smtp /var/qmail/bin/rblsmtpd

-r "blackholes.mail-abuse.org: Your

site has been listed in the MAPS RSS database"

/var/qmail/bin/qmail-smtpd

- با توجه به پیکربندی مورد بالا، از badmailfrom استفاده نشد، چون حاوی لیست عظیمی از دامنه‌های spammer می‌باشد.
- از ضد spamی بنام spamAssasin استفاده شد که هم حاوی لیست بزرگی از لغات spam است هم در کار خود، برترین می‌باشد[54].
- با توجه به پیکر بندی مورد بالا، دیگر نیازی به تعریف لغات نبود چون خود spamAssasin حاوی لیست عظیمی از لغات می‌باشد.
- حدود ۱۰۰ پست الکترونیکی spam ایجاد شد که از این ۱۰۰ پست الکترونیکی، ۱۳ مورد آن spam شناخته نشد.

گلوگاه[1] در spam، دو مسئله است: اول اینکه پیام‌ها را از سوی دامنه‌های spam مشهور نپذیرد[12]. ممکن است دامنه ای spammer باشد ولی در این لیست نیامده باشد. باید به این مسئله توجه داشت که spammer شدن و ثبت شدن در این لیست‌های جهانی، کار آسانی نیست. در ثانی ممکن است لغتی spam باشد ولی جزء لیست واژگان نباشد، یا اینکه spam نباشد ولی spam شمرده شود. احتمال موفقیت آمیز بودن مخاطره spam، با مکانیزم‌های بکار گرفته شده، وجود دارد. در آزمایشی که صورت گرفت، ۱۰۰ پست الکترونیکی spam ایجاد شد که ۱۳ مورد آن، حمله موفقیت آمیز بود.

---

[1] Bottleneck

جدول (٤-٥) : میزان کاهش مخاطره Spam

نام مخاطره	مخاطره Spam
شناسایی و محافظت	بلوکه کردن پیام‌هایی که از میزبان‌های spam شناخته شده می‌آید - بلوکه کردن پیام‌هایی که دربردارنده subject header تجاری شناخته شده، هستند – بلوکه کردن پیام‌هایی که در پایگاه داده spam جهانی، لیست شده‌اند.
تعداد آزمایش‌های صورت گرفته	١٠٠
تعداد حملات موفق	١٣
حملات نا موفق	٨٧
جمع امتیاز قبل از ایمن سازی	٤٣
میزان کاهش مخاطره(درصد)	٨٧
جمع امتیاز پس از ایمن سازی	٥.٥٩

۴-۱-۷ فیلتر کردن ویروس‌ها

مخاطره ویروس را در فصل سوم بررسی کردیم و در اهمیت پرداختن و مدیریت ویروس، مطالبی بیان کردیم. در این قسمت، راهکارهای مقابله ارائه می‌شود.

دو متد کلی برای انجام این کار وجود دارد[2]:

- فیلتر کردن بر اساس عبارات شناخته شده
- پویش[1] کردن فایل‌های پیوست

---

[1] scan

فیلتر کردن ویروس بر اساس عبارات شناخته شده

اساس این روش، بر این استوار است که بسیاری از ویروس‌ها، از عبارات خاصی درون سرآیند یا بدنه‌شان استفاده می‌کنند. این روش نقایصی دارد. مثلاً ویروس I LOVE YOU، ویروسی می‌باشد که در قسمت subject پیام، این عبارت را بکار می‌گیرد. حال اگر بخواهیم فیلترینگ، بر این اساس صورت گیرد، تمام پیام‌هایی که این عبارت را دارند، فیلتر می‌شوند و این مسئله، مناسب نیست. در ضمن، برخی از تولید کنندگان ویروس، عبارت‌های تصادفی ایجاد می‌کنند که شناخت آنها، سخت می‌باشد. ضرر دیگر این است که کاربر، دقیقاً پست الکترونیکی واقعی و سالم، دریافت کند که همان عبارت ویروس را داشته باشد. در نهایت اینکه برخی از مدیران پست الکترونیکی، ویروس‌هایی را فیلتر می‌کنند که فایل پیوست خاصی داشته باشند. این کار بر اساس MIME صورت می‌گیرد. اگرچه این روش، روش خوبی برای جلوگیری از ویروس می‌باشد، لکن کاربران را از ارسال فایل پیوست واقعی، محروم می‌کند و این نقطه ضعف بزرگی می‌باشد.

نقطه ضعف این روش، این است که بایستی از ویروس‌های جدید که هر روزه ایجاد می‌شوند، آگاهی یافت و عبارت خاصی را که درون این ویروس‌ها وجود دارد، به لیست فیلتر خود، اضافه کنید[2].

پویش کردن ویروس‌ها

استفاده از ضد ویروس[1]‌های تجاری، روش دوم متوقف کردن ویروس‌ها، بر روی سرور پست الکترونیکی می‌باشد.

پویش کردن پیام‌های پست الکترونیکی که حاوی ویروس هستند یا خیر، پروسه پیچیده تری از فیلتر کردن پیام‌ها می‌باشد[2]. این پروسه شامل مراحل زیر است:

۱. مشخص کردن اینکه آیا پیام پست الکترونیکی حاوی پیوست MIME یا uuencode هست یا خیر.

۲. استخراج فایل باینری از MIME یا uuencode.

[1] antivirus

۳. مشخص کردن اینکه آیا فایل فشرده شده است یا خیر. در صورت فشرده بودن، آن را به حالت اولیه برگردانیم.

٤. تمامی فایل‌های غیر فشرده را پویش کنیم.

۵. اگر فایل ویروسی نبود، اجازه دهیم که فایل به صورت نرمال، به گیرنده برسد و در غیر این صورت، گیرنده، مدیر محلی و فرستنده را مطلع کنیم.

همان‌طور که مشاهده می‌شود، قسمت اعظم این پروسه، بر روی پردازش فایل پیوست، تمرکز دارد. به همین دلیل برای سرورهایی که پیام‌های بسیار زیاد دریافت می‌کنند، این کار توصیه نمی‌شود.

مزیت عمده پویش ویروس این است که بسیاری از ویروس‌ها، امضای[1] خاصی دارند که بروز می‌شود. با بررسی این امضاها، به وجود ویروس پی می‌بریم.

پیاده سازی فیلترینگ ویروس

همان‌طور که ذکر شد سخت‌ترین قسمت فیلترینگ ویروس، پیدا کردن عبارت مناسبی است که ویروس از آن استفاده می‌کند. در جدول ٤-٦ برخی عبارات معروف برخی از ویروس‌ها را لیست کرده‌ایم[2]:

جدول (٤-٦) : برخی از عبارت‌های معروف ویروس‌ها[2]

Phrase	Virus
Subject: Homepage	VBS.VBSWG2.X@mm
Subject: Where are you?	VBS.Loveletter.CN@mm
Subject: Snow White and the Seven Dwarfs	W95.Hybris.gen
Subject: What is the seven sins?	VBS.Copy@mm
Subject: WindowsXP Betatest	VBS.Merlin.A@mm
Subject: Fw: Great & New Stuff 4 You!	VBS.Catfish@mm
Subject: Miss World	W32.MsWorld@mm

می‌توانید این عبارت‌ها را، از سایت‌های زیادی من جمله سایت شرکت Symantec، بدست آورید. همچنین می‌توانید برخی از فایل‌های پیوست با پسوند مشخص را فیلتر کنید. با فیلتر کردن پسوند فایل‌های اجرایی، از اجرا شدن برنامه ای روی سیستم سرور پست الکترونیکی، جلوگیری می‌کنید. در جدول ٤-٧ این مسئله را مشاهده می‌کنید[2].

---

[1] signature

جدول (٤-٧) :نوع فایل‌های اجرایی ممکن است ویروس باشند[2]

File Type	Description
.com	Microsoft executable files
.exe	Microsoft executable files
.vbs	Visual Basic script
.hlp	Microsoft help files
.pif	Microsoft Program Information File
.reg	Microsoft Registry file
.scr	Microsoft screen capture binary file
.shs	Shell automation code
.wsf	Microsoft Windows Scripting File
.sit	Apple Macintosh StuffIt format
.sea	Apple Macintosh self-extracting file

پیاده سازی پویش کردن ویروس

پیاده سازی پویش ویروس در بسته‌های MTA متن باز، امری پیچیده می‌باشد. در کنار نرم افزار MTA، دو نرم افزار اضافی مورد نیاز است:

- نرم افزار شناسایی و استخراج فایل‌های پیوست باینری از پیام‌های پست الکترونیکی.
- نرم افزار پویش فایل‌های باینری، برای شناخت ویروس‌های مشهور.

تعداد کمی از بسته‌های متن باز مختلف وجود دارند که می‌توانند پیوست‌های فایل‌های باینری را شناسایی کرده و استخراج کنند. بسته AMAVIS[1] که بسیار مشهور است می‌تواند فایل‌های پیوست را، از پیام‌ها استخراج کند، آنها را از حالت فشرده بیرون آورد و به نرم افزار ضد ویروس تحویل دهد تا آنها را پویش کند[55].

قسمت دیگر نرم افزاری که مورد نیاز است، نرم افزار ضد ویروس می‌باشد. نرم افزارهای ضد ویروس بسیار زیادی وجود دارد که برخی از آنها در جدول ٤-٨، لیست شده اند.

[1] A Mail Virus Scanner

جدول (٤-٨) :بسته‌های نرم افزاری ضد ویروس یونیکس[2]

Package	*Notes*
Network Associates Virus Scan	Version 3.x is available for free use, but is not supported. No new virus signature files are being created for this release (http://www.nai.com).
DrSolomon	This product has been discontinued; it is now part of the Network Associates product that has merged with McAfee (http://www.nai.com).
H+BEDV AntiVir/X	Free for noncommercial use, but requires registration (http://www.hbedv.com).
Sophos Sweep	30-day trial versions available (http://sophos.com).
Kaspersky Lab AVP	Supports only Linux systems (http://avp.ru).
Cybersoft Vfind	Standard Edition available for Unix systems (http://cyber.com).
Trend Micro FileScanner	Interscan Viruswall available for purchase for Unix systems (http://antivirus.com).
Computer Associates (CA) InoculateIT	30-day trial versions available (http://www.cai.com).

محاسبه میزان کاهش مخاطره

برای تست کاهش مخاطره، ضد ویروس ClamAV بر روی Qmail نصب شد[56]. نکته مهم در یک ضد ویروس، بروز بودن آن می‌باشد. بدیهی است که اگر این مسئله رعایت شده باشد، می‌توان گفت این مخاطره تقریباً به صفر تقلیل پیدا می‌کند. مگر آنکه ویروسی پیدا شود که ضد ویروس آن را نشناسد ولی این مورد نسبت به مواردی که ضد ویروس آن را می‌شناسد، بسیار ناچیز است و در نظر گرفته نمی‌شود[6].

جدول (٤-٩) : میزان کاهش مخاطره ویروس

نام مخاطره	مخاطره ویروس
شناسایی و محافظت	استفاده و نصب یک ضد ویروس قوی
تعداد آزمایش‌های صورت گرفته	با بروز بودن یک ضد ویروس، احتمال حمله تقریباً به صفر می‌رسد.
تعداد حملات موفق	۰
حملات نا موفق	با بروز بودن یک ضد ویروس، احتمال حمله تقریباً به صفر می‌رسد.
جمع امتیاز قبل از ایمن سازی	٤٧
میزان کاهش مخاطره(درصد)	۱۰۰
جمع امتیاز پس از ایمن سازی	۰

۴-۲ ایمن سازی سرویس پست الکترونیکی

در فصل سوم، مخاطراتی که برای سرویس پست الکترونیکی وجود دارند، بررسی شدند. در این قسمت راهکارها و مکانیزم‌های ایمن سازی این مخاطرات را بررسی می‌کنیم.

۴-۲-۱ استفاده از فایروال‌های پست الکترونیکی

نفوذکنندگان و spammerها، تکنیک‌های مختلفی استفاده می‌کنند تا اطلاعاتی در مورد سیستم پست الکترونیکی و کاربران آن بدست آورند. ولی تکنیک‌هایی وجود دارد که کمک می‌کند تا

با این مشکل مبارزه کنید. با غیر فعال کردن برخی دستورات و همچنین نصب دیوار آتش پست الکترونیکی، می‌توانید جلوی حملات و کاوشگری‌ها را بگیرید.

غیر فعال کردن برخی دستورات[2]

دستورHELO: به علت مسائل امنیتی، بسیاری از بسته‌های MTA بـه گونـه ای پیکـر بنـدی شده‌اند که از برقراری ارتباط بـا میزبـان‌هـایی کـه آدرس ip آنهـا، بـا اسـم میزبـان DNSی مناسب نگاشت نشود یا اسم میزبان DNS معکوسشان، با اسم میزبان ذکر شـده در دسـتور HELLO سازگار نباشد، ممانعت به عمل می‌آید.

دستورSEND: به علت تهدید امنیتی که در این دستور وجود دارد، اکثر بسته‌های نرم افزاری smtp، این دستور را فعال نمی‌کنند.

دستورSQML: به علت تهدید امنیتی کـه در ایـن دسـتور وجـود دارد، اکثـر بسـته‌هـای نـرم افزاریsmtp، این دستور را فعال نمی‌کنند.

دستورSAML : به علت تهدید امنیتی که در ایـن دسـتور وجـود دارد، اکثـر بسـته‌هـای نـرم افزاری smtp این دستور را فعال نمی‌کنند.

دستورVRFY: به علت تهدید امنیتی کـه در ایـن دسـتور وجـود دارد، اکثـر بسـته‌هـای نـرم افزاریsmtp، این دستور را فعال نمی‌کنند.

دستورTURN: این دستور به علت مسائل امنیتی در سرورهای امروزی، استفاده نمی‌شود.

دستور EXPN: به علت تهدید امنیتی که در ایـن دسـتور وجـود دارد، اکثـر بسـته‌هـای نـرم افزاریsmtp، این دستور را فعال نمی‌کنند.

ردیابی سرآیندها[1]

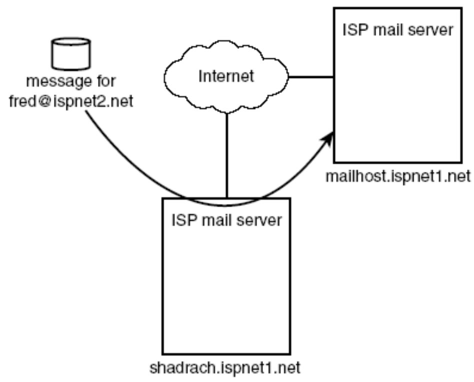
یکی از بزرگ‌ترین مشکلات در مورد ردیابی پیام‌های پست الکترونیکی، تعامل با سرآیند پست الکترونیکی‌های جعلی می‌باشد.

این بخش به برخی تکنیک‌هایی که مدیران پست الکترونیکی می‌توانند سرآیندهای پست الکترونیکی را بخوانند یا فرستنده پست الکترونیکی را ردیابی کنند، می‌پردازد[28].

[1] headers

فیلد سرآیند Received

Spammerها بندرت پیام‌ها را مستقیماً به قربانیانشان می‌فرستند. آنها معمولاً از یک سرور پست الکترونیکی واسط، بهره می‌گیرند تا ردیابی آنها را سخت‌تر کند. در شکل ٤-٥ این مسئله را مشاهده می‌کنید.



شکل (٤-٥) : ارسال پیام‌های جعلی از یک سرور میانی

هنگامی‌که یک سرور پست الکترونیکی، یک پیام را می‌گیرد، قبل از اینکه آن را تحویل پست الکترونیکی سرور بعدی یا کلاینت بدهد، به آن فیلد received اضافه می‌کند. این فیلد کمک می‌کند تا فرستنده را ردگیری کنید[28]. در جدول ٤-١٠ پارامترهای فیلد received را ذکر کرده‌ایم.

جدول (٤-١٠) : پارامترهای فیلد received [28]

پارامتر	توضیح
From host_name	میزبان ارسال کننده پیام
By host_name	میزبان دریافت کننده پیام
Via physical path	چگونه پیام فرستاده شده است.
With protocol	پروتکلی که برای ارسال پیام از آن استفاده شده است.
Id message_id	یک شناسه پیام منحصربه‌فرد برای گیرنده
For final_e-mail_destination	آدرس پست الکترونیکی گیرنده

به عنوان مثال در کد زیر، netposta.net پست الکترونیکی سرور مجرم می‌باشد و moon1.kimo.com، پست الکترونیکی سرور relay می‌باشد.

Return-Path: <alfki@miesto.sk>

Received: from moon1.kimo.com.tw (sourcenat1.bigmailbox.com

➥ [209.132.220.250])

by mailrecv22.bigmailbox.com (8.10.0/8.10.0) with ESMTP id f3L9Eex32005;

Sat, 21 Apr 2001 02:14:41 -0700

Received: from netposta.net ([208.187.10.89]) by

moon1.kimo.com.tw (Netscape Messaging Server 4.15) with SMTP id

GC3CG500.F3W; Fri, 20 Apr 2001 20:38:29 +0800

Message-ID: <00000ad359dd$00003352$000076da@netposta.net>

To: <173@artic.net>

From: alfki@miesto.sk

Subject: FW:

Date: Thu, 19 Apr 2001 18:52:52 -0800

MIME-Version: 1.0

Content-Type: text/html;

charset=”iso-8859-1”

Content-Transfer-Encoding: quoted-printable

X-Priority: 3

X-MSMail-Priority: Normal

Attachments: msg1.html

فیلد سرآیند Message-Id

برخی بارها شاید نیاز نباشد که فیلد received را دنبال کنید، فیلد message id اطلاعات نام دامنه و برخی بارها، کاربر ارسال کننده را نشان می‌دهد[28]. در کد زیر، نام دامنه مشخص است.

Message-ID: <00000ad359dd$00003352$000076da@netposta.net>

در ادامه، با دانستن نام دامنه می‌توانید اطلاعات مشروح‌تری درباره مجرم یا ISP[1] آن بدست آورید. با ابزارهایی چون whois، nslookup و dig می‌توان این کار را انجام داد. در نهایت می‌توانید با روش‌های ممانعت از spam، جلوی این‌گونه پست الکترونیکی‌ها را بگیرید.

فایروال‌های پست الکترونیکی

همان‌طور که گفته شد، اگر دستور VRFY غیر فعال شده باشد از RCPT TO استفاده می‌شود. در اینجا برای جلوگیری از RCPT TO از دیوار آتش پست الکترونیکی، استفاده می‌کنیم[12].

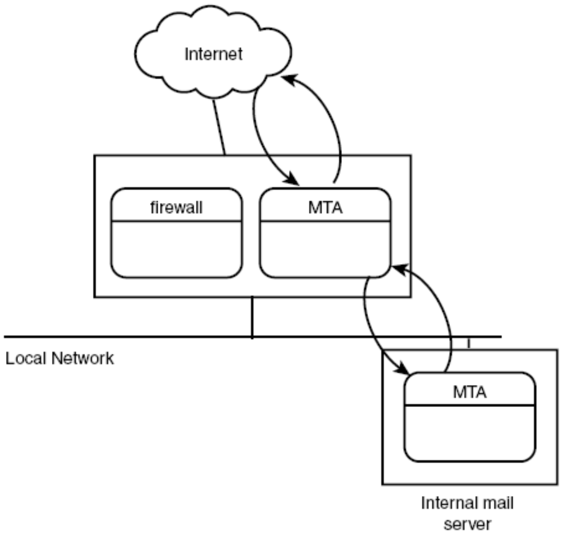
یک فایروال پست الکترونیکی، یک سرور پست الکترونیکی می‌باشد که هدف آن این است که پیام‌های ورودی و خروجی از و به سرور داخلی را، بپذیرد یا رد کند. فایروال پست الکترونیکی به گونه ای پیکربندی شده است که پیام‌های دامنه را بپذیرد و آنها را به سمت پست الکترونیکی سرور دامنه حقیقی بفرستد. برای محل فایروال، سه گزینه پیش رو دارید که به شرح آن‌ها پرداخته‌ایم.

درون فایروال شبکه

آسان‌ترین راه پیاده سازی این است که فایروال پست الکترونیکی را درون همان سرور قرار دهیم[2]. در شکل ٤-٦ این مسئله را مشاهده می‌کنید. مزیت این روش، استفاده از تعداد کمتری سرور، نسبت به دیگر متدها می‌باشد و علت آن استفاده از فقط یک سرور، هم برای فایروال شبکه هم برای فایروال پست الکترونیکی می‌باشد.

---

[1] Internet Service Provider



شکل (٤-٦) :قرار دادن فایروال پست الکترونیکی بر روی سرور فایروال شبکه

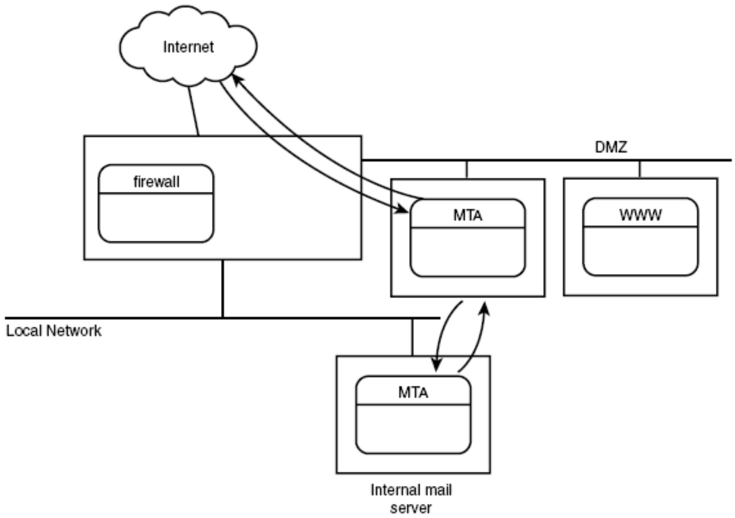
وقتی این متد را انتخاب میکنید، بایستی مطمئن باشید که فایروال شبکه، توانایی پردازش هر دو کار را دارد یا خیر. بسیاری از مدیران پست الکترونیکی و شبکه، این کار را به صورت سعی و خطا انجام می‌دهند که این کار برای کاربران اذیت کننده می‌باشد.

درون DMZ[1]

راه حل پیچیده تر نسبت به راه حل بالا، قرار دادن فایروال پست الکترونیکی درون DMZ می‌باشد. DMZ یک شبکه مخصوص است که درون فایروال پیکربندی می‌شود و از هر دو شبکه بیرونی و درونی مجزا شده است[2]. فایروال مسئول اجازه دادن به ترافیک‌های مخصوص شبکه ای، به درون و بیرون از DMZ می‌باشد. به صورت معمول، فایروال به گونه ای پیکربندی می‌شود که دسترسی خارجی به میزبان‌های درون DMZ را می‌دهد، در حالی که دسترسی به شبکه داخلی را محدود میکند. سرورهایی مانند سرور پست الکترونیکی، سرور وب و سرور FTP، که به صورت مداوم توسط کاربران خارجی، مورد دسترسی قرار می‌گیرند معمولاً درون DMZ قرار می‌گیرند. شکل ٤-٧ این مسئله را نشان می‌دهد. اگر چه این متد، امنیت سفت و سختی بر روی پست الکترونیکی سرور ایجاد می‌کند، اما پیکربندی پیچیده ای برای فایروال، نیاز دارد. DMZ بایستی به صورت بسیار دقیقی

[1] Demilitarized Zone

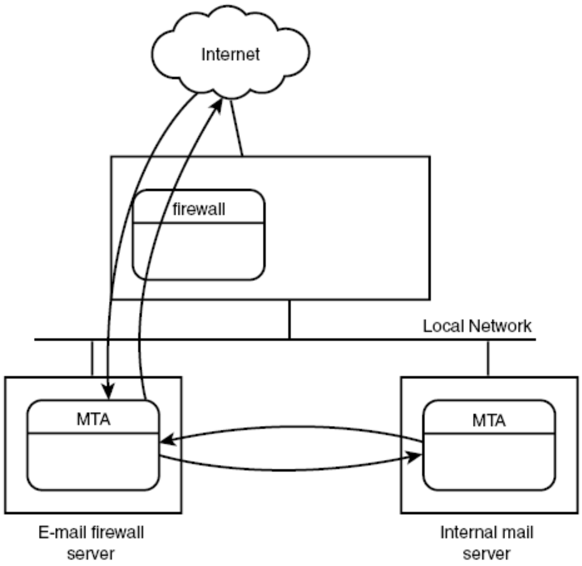
مانیتور شود تا مطمئن شویم ترافیکی که از اینترنت وارد می‌شود، به شبکه درونی آسیب نمی‌رساند.



شکل (٤-٧) : قرار دادن سرور فایروال پست الکترونیکی درون DMZ

به عنوان یک سرور پست الکترونیکی داخلی

متد دیگر، قرار دادن فایروال پست الکترونیکی اختصاصی بر روی سرورهای مجزا، درون شبکه محلی نرمال در طول سرور پست الکترونیکی درونی می‌باشد[2]. فایروال شبکه بایستی به گونه ای پیکربندی شود تا اجازه دهد ترافیک‌های شبکه مناسب، به شبکه محلی راه یابد تا با فایروال پست الکترونیکی متصل شود در حالی که دسترسی به سرور پست الکترونیکی درونی را مسدود کرده‌ایم. شکل ٤-٨ این مسئله را نشان می‌دهد. در این متد سرور فایروال، بایستی بدقت پیکربندی شود تا ترافیک‌های POP، IMAP و SMTP را از اینترنت، فقط به فایروال پست الکترونیکی مجاز کند، نه هر میزبان دیگری که بر روی شبکه داخلی قرار گرفته است.



شکل (۴-۸) :استفاده از یک سرور پست الکترونیکی درونی

محاسبه میزان کاهش مخاطره

برای تست کاهش مخاطره دو مطلب حائز اهمیت است:

Qmail به صورت پیش فرض، دستورات دارای مخاطره را غیر فعال کرده است.

- در iptables قواعد مناسبی نوشته شد و جلوی دسترسی‌های اضافی، بجز smtp گرفته شد.

ipchains -P forward DENY/sbin/ipchains -A forward -i ppp0 -j MASQ

ipchains -A input -I ppp0 --destination-port smtp -y -j ACCEPT

ipchains -A input -i ppp0 -l -y -j DENY

- فایل‌های log، در هر حمله بررسی شدند و به ازای حملات در iptables و ipchains یک قاعده، اضافه شد.
- حملات با ipهای مختلفی انجام شد.
- حملات برای ۱۰۰۰ نمونه اجرا شد.

- برای تست، سعی شد به سرویس‌های مختلف، اتصال ایجاد شود، اما چون در iptables و ipchains جلوی آن‌ها گرفته می‌شد، deny رخ می‌داد و حمله صورت نمی‌گرفت.

Unable to connect to remote host: Connection refused

نتیجه آزمایش بدین صورت بود که با اعمال موارد فوق، از ۱۰۰۰ حمله، هیچ حمله ای موفقیت آمیز نبود. یعنی جمع امتیاز مخاطره، پس از این کار به صفر رسید.

جدول (٤-۱۱) :میزان کاهش مخاطره سوء استفاده از برخی دستورات و کاوش گری

نام مخاطره	مخاطره سوء استفاده از برخی دستورات و کاوش گری
شناسایی و محافظت	غیر فعال کردن دستورات پرمخاطره – نصب فایروال
تعداد آزمایش‌های صورت گرفته	۱۰۰۰
تعداد حملات موفق	۰
تعداد حملات نا موفق	۱۰۰۰
جمع امتیاز قبل از ایمن سازی	۲۳
میزان کاهش مخاطره(درصد)	۱۰۰
جمع امتیاز پس از ایمن سازی	۰

۴-۲-۳ استفاده از SASL[1]

در فصل مخاطرات، درباره open relay بحث شد و گفته شد که هدف، ایجاد رله گزینشی می‌باشد. متدهایی که ذکر شد بر اساس آدرس ip یا نام میزبان بود. اما متأسفانه این‌گونه

---

[1] Simple Authentication and Security Layer

نیست که در عمل، تمامی کاربران از آدرس ip مخصوص و معینی استفاده کنند تا بتوان آنها را درون جدول relay تعریف کرد. متد رایج دیگر، اجازه دادن به میزبان‌های راه دور که بتوانند پیام‌ها را از طریق پست الکترونیکی سرور، رله کنند، استفاده از یک متد تایید هویت می‌باشد. متد تایید هویت به صورت منحصربه‌فرد می‌تواند پست الکترونیکی سرور راه دور را مشخص کند، به نحوی که سرور پست الکترونیکی بتواند مشخص کند اجازه دارد پیام‌ها را رله کند یا خیر[7].

یکی از مشهورترین متدهای تایید هویت اتصالات شبکه، SASL می‌باشد[8]. این پروتکل یک مجموعه از مکانیسم‌های تایید هویت را مشخص می‌کند که هر برنامه کاربردی شبکه می‌تواند از آن استفاده کند تا هویت کاربران راه دور را تایید کند. بسیاری از بسته‌های MTA متن باز[1]، از SASL استفاده می‌کنند تا دستور AUTH را پیاده سازی کنند. این دستور، به میزبان‌های smtp اجازه می‌دهد تا از تایید هویت کلاینت درون یک جلسه smtp استفاده کنند[57].

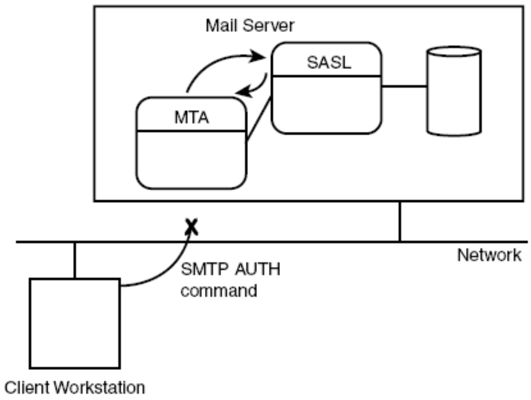
SASL چیست؟

SASL برای مهیا کردن مکانیسم تایید هویت، برای کاربردهای شبکه ای که از دستورات کلاینت/سرور استفاده می‌کنند، مانند POP3، IMAP و SMTP، به‌کار می‌رود[8][7].

SASL چگونه عمل می‌کند؟

SASL درون کاربرد شبکه[2] عمل می‌کند و یک API[3] را مهیا کرده است که می‌تواند برای ارزیابی، هنگام تلاش‌های تایید هویت کلاینت راه دور، مورد استفاده قرار گیرد[8]. شکل ٤-٩ این مسئله را نشان می‌دهد.

[1] Open source
[2] Network application
[3] Application Programming Interface



شکل (٤-٩) :استفاده از sasl درون یک کاربرد شبکه

کاربرد شبکه، بایستی متدی برای پذیرفتن یک نشانه تایید هویت، از کلاینت شبکه راه دور فراهم کند. این مسئله معمولاً با دستور متنی، همانند Smtp AUTH انجام می‌شود. نشانه تایید هویت، سپس به لایه sasl برای ارزیابی، تحویل داده می‌شود. اگر نتیجه ارزیابی درست بود، آنگاه sasl یک پاسخ مثبت، به کاربرد بر می‌گرداند و کلاینت شبکه راه دور، اجازه دارد از کاربرد شبکه استفاده کند. در غیر این صورت، پاسخ منفی برگشت داده می‌شود و کلاینت راه دور شبکه، اجازه استفاده از کاربرد شبکه را پیدا نمی‌کند. البته قابل ذکر است که sasl از متد رمزنگاری، استفاده نمی‌کند و فقط برای تایید هویت بکار می‌رود. برای رمزنگاری بایستی از ssl[1] استفاده کرد.

مکانیزم‌های تایید هویت SASL

مکانیزم‌های فراوانی برای تایید هویت کاربر، درون ساختار sasl موجود است[8]. سه مکانیزم مشهور در زیر آورده شده است.

KERBEROS: کلاینت، از بلیط Kerberos برای تایید هویت، استفاده می‌کند.

GSSAPI: کلاینت، نام کاربری و گذر واژه کدگذاری شده بر اساس GSSAPI می‌فرستد.

SKEY: کلاینت، نام کاربری کدگذاری شده ٦٤ بیتی و گذرواژه یک‌بار مصرف می‌فرستد.

---

[1] Secured socket layer

مکانیزم‌های دیگری همچون CRAM_MD5، DIGEST_MD5، PLAIN TEXT و LOGIN هم وجود دارد.

استفاده از SASL درون SMTP

دستور AUTH، به صورت یک دستور مجزا یا همراه با دستور MAIL FROM می‌تواند استفاده شود[8]. فرمت دستور AUTH به صورت زیر است:

AUTH Mechanism

نکته مهم این است که در استفاده از smtp بایستی از ESMTP و دستور EHLO استفاده کنید تا دستور AUTH را پشتیبانی کند. لیست زیر، نمونه ای از استفاده از این دستور را نشان می‌دهد.

$ **telnet localhost 25**

Connected to localhost.

220 shadrach.ispnet1.net ESMTP sendmail 8.11.3/8.11.3; Thu, 5 Apr 2001 09:12:36 -00

EHLO shadrach.ispnet1.net

250-shadrach.ispnet1.net Hello IDENT:rich@localhost [127.0.0.1], pleased to meet you

250-ENHANCEDSTATUSCODES

250-EXPN

250-VERB

250-8BITMIME

250-SIZE

250-DSN

250-ONEX

250-ETRN

250-XUSR

250-AUTH LOGIN DIGEST-MD5

250 HELP

AUTH LOGIN

334 VXNlcm5hbWU6

cmljaA==

334 UGFzc3dvcmQ6

cHJsbmpn

235 2.0.0 OK Authenticated

MAIL FROM: rich@shadrach.ispnet1.net

250 2.1.0 rich@[158.18.1.153]... Sender ok

RCPT TO: richard.blum@meshach.ispnet2.net

250 2.1.5 richard.blum@meshach.ispnet2.net... Recipient ok

DATA

354 Enter mail, end with "." on a line by itself

Subject: test

From: rich@shadrach.ispnet1.net

To: richard.blum@meshach.ispnet2.net

This is a test message.

.

250 2.0.0 f35EDFB04406 Message accepted for delivery

QUIT

Connection closed by foreign host.

محاسبه میزان کاهش مخاطره

با توجه به اینکه استفاده کردن از SASL در مخاطره Open Relay کاربرد دارد و مهم‌ترین کار در آزمایش این است که پیام‌ها را از سرورهای open relay مشهور نپذیرید، پیکربندی SASL، تأثیر چندانی در محاسبه کاهش مخاطره SASL ندارد و می‌توان همان جدول کاهش مخاطره را ارائه داد.

جدول (٤-١٢) : میزان کاهش مخاطره open relay

نام مخاطره	مخاطره Open Relay
شناسایی و محافظت	پیام‌ها را از سرورهای open relay مشهور نپذیرید- با توجه به رله گزینشی، مشخص می‌کنیم که پیام‌ها را به کدام سرورها رله کند
تعداد آزمایش‌های صورت گرفته	۱۰۰
تعداد حملات موفق	۲۰
حملات نا موفق	۸۰
جمع امتیاز قبل از ایمن سازی	۳۲
میزان کاهش مخاطره(درصد)	۸۰
جمع امتیاز پس از ایمن سازی	٦.٤

S-MIME ۴-۲-۴

S-MIME به این منظور ایجاد شد که راهی ایجاد کند تا پیام‌ها را به صورت امن در اینترنت ارسال شوند. کد گذاری که در MIME برای انتقال فایل‌های باینری ایجاد شده بود، برای پیام‌ها، امنیتی ایجاد نمی‌کرد، چون با یک کدگشا قابل باز شدن بود. S-MIME علاوه بر کدگذاری، از رمزنگاری برای ایجاد امنیت در پیام‌ها استفاده می‌کند[42].

S-MIME Multipart SubType

زیر نوع امضا شده پیام، شامل دو بخش است: پیام استاندارد و امضای دیجیتالی. این متد پیام اصلی را رمزنگاری نمی‌کند بنابراین خوانندگان پست الکترونیکی، فاقد قابلیت S-MIME، قادر به خواندن پیام هستند[42]. کد گذاری که برای فایل باینری ایجاد می‌شود معمولاً متد base64 می‌باشد.

Content-Type: multipart/signed;

protocol=”application/pkcs7-signature”;

micalg=sha1; boundary=boundary42

--boundary42

Content-Type: text/plain

This is a clear-signed message.

--boundary42

Content-Type: application/pkcs7-signature; name=smime.p7s

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6

4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj

n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4

7GhIGfHfYT64VQbnj756

--boundary42--

پارامترهای protocol و micalg پروتکل مورد استفاده برای تولید امضای دیجیتال را مشخص می‌کند.

برای حفاظت از پست الکترونیکی از دیدگاه امنیتی، بایستی از یک تابع فرعی دیگر S-MIME، بنام S-MIME Application SubType بهره برد[42].

S-MIME Application SubType

زیر نوع Pkcs-mime application، ویژگی‌های امنیتی بسیار متفاوتی برای ایجاد امنیت در پیام، ایجاد می‌کند. این ویژگی‌ها در s-mime type مشخص می‌شوند[42]. فرمت کار به صورت زیر می‌باشد.

Content-Type: application/pkcs7-mime; smime-type=*feature*;name=*filename*

Filename اسم فایلی می‌باشد که داده‌ها باید در آنجا ذخیره شوند. جدول ٤-۱۳ ویژگی‌های امنیتی که توسط pkcs-mime می‌توانید بکار ببرید مشخص می‌کند.

جدول (٤-۱۳) : ویژگی‌های pkcs-mime

ویژگی	توضیح
data	متن پیام رمزگذاری نشده
Encrypted-data	متن پیام رمزگذاری شده
Signed-data	متن پیام رمزگذاری نشده بعلاوه یک امضای دیجیتال
Enveloped-data	متن پیام رمزگذاری شده
Signed-and-enveloped-data	متن پیام رمزگذاری شده بعلاوه یک امضای دیجیتال
Digest-data	متن پیام hash شده که برای تعیین هویت پیام اصلی، بکار می‌رود.

MIME به همراه PGP

در کنار S-MIME، بسیاری از بسته‌های پست الکترونیکی، بسته‌های امنیتی و ویژگی‌های امنیتی فراوانی را در RFC-822 معرفی کرده اند. یکی از بسته‌های امنیتی رایج، PGP[1] می‌باشد.

بسته pgp به منظور امضا و رمز نگاری پیام، به وجود آمده است که بسیاری از الگوریتم‌های امنیتی استاندارد را پشتیبانی می‌کند[43]. بسته pgp از جفت کلید عمومی و خصوصی استاندارد استفاده می‌کند. این بسته، کاربر را قادر می‌سازد یک فایل را توسط

[1] Pretty Good Privacy

کلید خصوصی امضا کند و کاربران راه دور را قادر می‌سازد که آن را توسط کلید عمومی، تایید هویت کند. هنگامی که یک کاربر، فایل را رمز نگاری می‌کند، این کار را با کلید عمومی گیرنده، انجام می‌دهد تا گیرنده بتواند آن را با کلید خصوصی‌اش باز کند.

بسته‌های pgp برای کاربران غیر تجاری، به صورت رایگان وجود دارد ولی برای کاربران تجاری، بایستی مبلغی پرداخت شود. به خاطر این هزینه، بسیاری از بسته‌های پست الکترونیکی، pgp را در خود پیاده سازی نمی‌کنند. برای پشتیبانی pgp، کاربر قبل از اینکه بخواهد پیام خود را ارسال کند، بایستی آن را رمزنگاری کند. آنگاه بسته pgp، آن را به base-64 کدگذاری می‌کند. حال، پیام می‌تواند به صورت مستقیم ارسال شود.

محاسبه میزان کاهش مخاطره

در آزمایش صورت گرفته در هنگام ارسال پیام، از پروتکل s-mime استفاده شد. از ۱۰۰ پیام فرستاده شده، هیچ یک قابل خواندن نبود و پیام ایمن بود. برای انجام این تست، از نرم‌افزار ethereal استفاده شد تا پیام‌ها را capture کنیم.

جدول (۴-۱۴) : میزان کاهش مخاطره نا امن بودن محتوی پیام

نام مخاطره	مخاطره ناامن بودن محتوی پیام
شناسایی و محافظت	استفاده از s-mime
تعداد آزمایش‌های صورت گرفته	۱۰۰
تعداد حملات موفق	۰
حملات نا موفق	۱۰۰
جمع امتیاز قبل از ایمن سازی	۲۶
میزان کاهش مخاطره(درصد)	۱۰۰
جمع امتیاز پس از ایمن سازی	۰

۴-۲-۵ امن کردن سرورهای POP3 و IMAP

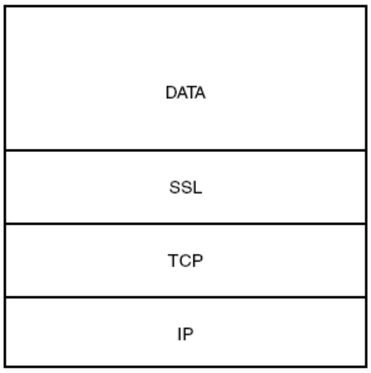
بسیاری از بسته‌های MTA، برای دریافت پیام‌ها از پروتکل‌های pop3 یا imap بهره می‌گیرند. مشکل این پروتکل‌ها این است که آنها اطلاعات را به صورت متن اسکی، بدون هیچ رمز نگاری ارسال می‌کنند. برای کمک کردن به این‌گونه مسائل پروتکل SSL[1] به وجود آمد که به میزبان‌های شبکه، اجازه می‌دهد تا داده‌ها را قبل از ارسالشان در طول شبکه، رمز کنند.

پروتکل‌های خانواده SSL

پروتکل SSL توسط شرکت Netscape ایجاد شد و پس از سال‌ها، اصلاحیه‌های متفاوتی برای آن ایجاد شد. پس از اینکه نسخه سوم پروتکل SSL ایجاد شد، پروتکل دیگری که مشابه SSL می‌باشد، معرفی گشت و نام آن پروتکل، TLS[2] نهاده شد[11]. TLS کاملاً با SSL سازگار است و بجای آن نیز استفاده می‌شود.

پروتکل SSL

پروتکل SSL مابین لایه TCP/IP و کاربرد قرار دارد. شکل ٤-١٠ نشان می‌دهد که SSL چگونه در لایه‌های شبکه قرار می‌گیرد[11].



شکل (٤-١٠) :پروتکل ssl در ارتباط با tcp/ip

در پروتکل SSL، هر کلاینت می‌تواند یک جلسه SSL با سرور راه دور داشته باشد و سپس می‌تواند چندین اتصال یا کاربرد شبکه، درون یک جلسه داشته باشد.

1 Secured Socket layer
2 Transport Layer Security

جلسه SSL، مسئول ایجاد و نگهداری یک محیط امن، برای اتصالات است، به گونه ای که تایید هویت ارسال کننده داده ارسالی را، نیز انجام می‌دهد.

جدول ٤-۱۵ عناصر کلیدی که در جلسه SSL بکار می‌رود را، لیست کرده است[11].

جدول (٤-۱۵) : عناصر کلیدی جلسه ssl

عنصر	توضیح
Identifier	ترتیب بایت دلخواهی، که وضعیت جلسه را نشان می‌دهد.
Certificate	گواهی X.509 که سرور را مشخص می‌کند.
Compression	متد فشرده سازی کاربرد، قبل از رمزنگاری
Cipher	الگوریتم رمزنگاری که داده کاربرد موجود در بسته ssl را تایید هویت می‌کند.
Secret	کد ٤٨ بایتی که بین کلاینت و سرور، برای الگوریتم رمز نگاری قرار داده اند.
Resumable	یک پرچم که نشان می‌دهد یک جلسه از قبل، ادامه می‌یابد یا خیر.

پروتکل ssl خود از دو بخش مجزا، تشکیل شده است:

- پروتکل هسته ای که داده‌های ssl را ارسال و دریافت می‌کند.
- مجموعه ای از بسته‌های کنترلی که جلسه ssl را کنترل می‌کند.

ssl پروتکل هسته ای را به عنوان پروتکل رکورد، معرفی می‌کند. این همان جایی است که امنیت و یکپارچگی داده اتفاق می‌افتد.

بسته‌های کنترلی به منظور کمک کردن به ایجاد، مدیریت و بستن جلسه ssl بکار می‌رود. سه بسته کنترلی در زیر لیست شده‌اند.

- پروتکل دست دهی
- پروتکل تغییر مشخصات رمز
- پروتکل هشدار

پروتکل Record SSL

هر بسته sslی که در طول شبکه منتقل می‌شود، به عنوان یک رکورد، در نظر گرفته می‌شود. پروتکل رکورد ssl، پنج وظیفه را برای جلسه ssl فراهم می‌کند[11].

Fragmentation: بسته‌های بزرگ را به بسته‌های با سایز ١٦٣٨٤ بایت، تبدیل می‌کند.

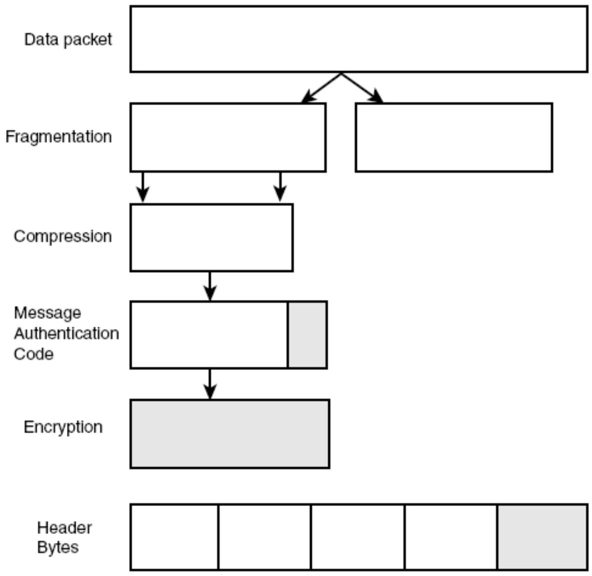
Compression: فشرده سازی می‌تواند بر روی پیام کلاینت تکه تکه شده، اعمال شود.

Message authentication: یک MAC، برای پیام فشرده شده توسط یک کلید محرمانه تسهیم بندی شده، محاسبه می‌شود. MAC، کلاینت را قادر می‌سازد تا سرور را ارزیابی کند.

Message encryption: داده فشرده شده حاصله و بسته MAC، رمز می‌شوند تا امنیت را در طول شبکه فراهم کنند.

Header Bytes: سرآیند ٤٠ بیتی برای بسته رمز شده، مهیا شده است.

در شکل ٤-١١، این وظایف را درون یک پروتکل رکورد ssl نشان داده‌ایم.



شکل (٤-١١) : پروتکل رکورد ssl

پروتکل دست دهی[1] SSL

پروتکل دست دهی ssl، کلاینت و سرور را قادر می‌سازد تا درباره پارامترهای جلسه، مذاکره کنند. این پروتکل از ۱۰ پیام مختلف برای این کار استفاده می‌کند[11]. جدول ٤-١٦ لیستی از بسته‌های پیام این پروتکل را آورده است.

جدول (٤-١٦) : پیام‌های مختلف پروتکل دست دهی ssl

هشدار	توضیح
Hello_request	توسط سرور ارسال می‌شود تا کلاینت را وادار کند پروتکل دست دهی را شروع کند.
Client_hello	توسط کلاینت ارسال می‌شود تا پروتکل ssl را آغاز کند. لیستی از پروتکل‌های رمز نگاری و فشرده سازی را برای کلاینت ارائه می‌دهد.
Server_hello	پاسخ سرور به client_hello می‌باشد و همچنین لیستی از پروتکل‌های رمز نگاری و فشرده سازی را داراست که توسط کلاینت مشخص شده است.
certificate	توسط سرور ارائه می‌شود تا خود را به کلاینت بشناساند.
Server_key_exchange	اگر سرور گواهی نداشته باشد کلید عمومی‌اش را ارسال می‌کند.
Certificate_request	سرور تقاضای گواهی کلاینت را می‌کند.
Server_hello_done	انتهای پیام hello سرور را مشخص می‌کند.
Client_certificate	توسط کلاینت ارسال می‌شود، اگر سرور پیام certificate_request ارسال کند.
Client_key_exchange	توسط کلاینت ارسال می‌شد تا کلید عمومی که برای رمزگشایی پیام‌های رمز شده استفاده می‌شود، را مشخص کند.
Certificate_verify	توسط کلاینت ارسال می‌شود تا گواهی ارسالی توسط کلاینت را ارزیابی کند.
finished	بعد از بسته تغییر پروتکل رمزنگاری، ارسال می‌شود تا

[1] handshake

مشخص کند که پروسه به خوبی انجام گرفته است.

پروتکل تغییر مشخصات رمز SSL

پروتکل تغییر مشخصات رمز، به منظور فرستادن سیگنال، به تغییرات در رمز استفاده می‌شود و در طول جلسه فعال ssl استفاده می‌شود[11]. این متد اغلب برای افزایش امنیت اتصال، بکار می‌رود. تغییر دادن رمز، در طول اتصال، شکستن رمز و بدست آوردن داده را برای اشخاص، بسیار سخت می‌کند.

پروتکل هشدار دهنده SSL

این پروتکل کلاینت و سرور را قادر می‌سازد تا همتاهایشان را از وجود اشکال در جلسه ssl، آگاه کنند[11]. جدول ٤-١٧ این پیام‌ها را لیست کرده است.

جدول (٤-١٧) : پیام‌های مختلف پروتکل هشدار دهنده ssl

هشدار	توضیح
Bad_certificate	گواهی دریافتی، خراب است.
Bad_record_match	رکورد دریافتی، MAC اش خراب است.
Certificate_expired	گواهی منقضی شده است.
Certificate_revoked	گواهی لغو شده است.
Certificate_unknown	گواهی به دلایل دیگر رد شده است.
Close_notify	اتصال بسته شده است.
Decompression failure	از حالت فشرده در آوردن فایل فشرده، با اشکال مواجه شده است.
Handshake_failure	مذاکره بین پارامترهای موجود در دست دهی، با اشکال مواجه شده است.
Illegal_parameter	فیلدی درون پارامترهای دست دهی، اشکال دارد.
No_certificate	گواهی موجود نیست.
Unexpted message	یک پیام نامرتبط، دریافت شده است.
Unsopported certificate	نوع گواهی درست نیست.

پروتکل TLS

پروتکل TLS در واقع تغییریافته پروتکل SSL نسخه ۳ می‌باشد[44]. تمامی ویژگی‌هایی که برای SSL ذکر شد، برای TLS هم وجود دارد. این پروتکل ویژگی‌های زیادی را بر روی SSL، برای خود گسترش داده است. TLS ویژگی‌های جزیی بسیار زیادی را بهبود داده است، مانند الگوریتمی که برای محاسبه مقدار MAC استفاده می‌شود. نوع‌های هشدار هم، افزوده شده است. در جدول ٤-١٨ این نوع هشدارهای اضافه شده، نشان داده شده است.

جدول (٤-١٨) : پیام‌های مختلف پروتکل هشدار دهنده TLS [44]

هشدار	توضیح
Access_denied	یک گواهی معتبر، دریافت می‌شود ولی فرستنده، دسترسی‌اش بسته شده است.
Decode_error	پیامی که به علت یک خطا درون یک فیلد، نمی‌تواند کدگشایی شود.
Decrypt_error	یک دست دهی رمزنگاری، رد شده است.
Decryption_field	دریافت کننده، نمی‌تواند پیام رمز شده را رمزگشایی کند.
Export_restriction	مذاکرات رمزنگاری، به خاطر محدودیت انجام نشده است.
Insufficient_security	سرور، یک رمز را در سطح بالاتر امنیتی، درخواست می‌کند.
Internal_error	یک خطای درونی نامرتبط با همتا، شناسایی شده است.
No_renegotiations	فرستنده قادر نیست جلسه را باز مذاکره کند.
Protocol_version	نسخه پروتکل مذاکره شده، معتبر نیست.
Record_overflow	یک رکورد TLS دریافت شده است که طولش از حداکثر مجاز تجاوز کرده است.
Unknown_ca	یک گواهی معتبر دریافت شده، ولی CAS گواهی، با یک CA قابل اعتماد، تطابق ندارد.
User_canceled	دست دهی لغو شده است.

بسته OpenSSL

بسته openssl محبوب‌ترین متدی است که با برنامه‌های متن باز استفاده می‌شود تا قابلیت SSL را برای آنها ایجاد کند. در استفاده از ssl از گواهی‌ها بهره می‌گیریم[12]. دستور زیر نحوه استفاده از openssl را نشان می‌دهد.

openssl req -new -x509 -nodes -out imapd.pem -keyout imapd.pem -days 3650

این دستور، یک گواهی با پروتکل x509 ایجاد می‌کند و نام آن را imapd.pem قرار می‌دهد. هر دو کلید خصوصی و گواهی را در یک فایل، قرار می‌دهد و آن را برای ۳٦۵۰ روز، اعتبار می‌دهد.

پس از این مرحله، بایستی بسته MTA خود را، طوری پیکربندی کنید تا از ssl استفاده کند. مثال زیر، نحوه استفاده بسته MTAای بنام UW را، از ssl نشان می‌دهد. این بسته از پورت ۹۹۵ برای pop3 به همراه ssl، استفاده می‌کند. این تست بر روی سرور، انجام شده است.

$ **/usr/local/ssl/bin/openssl s_client -host localhost -port 995**

CONNECTED(00000003)

depth=0 /C=US/ST=Indiana/L=Indianapolis/O=E-mail book/OU=Chapter 16/

➥CN=shadrach.ispnet1.net

verify error:num=18:self signed certificate

verify return:1

depth=0 /C=US/ST=Indiana/L=Indianapolis/O=E-mail book/OU=Chapter 16/

➥CN=shadrach.ispnet1.net

verify return:1

--

Certificate chain

0 s:/C=US/ST=Indiana/L=Indianapolis/O=E-mail book/OU=Chapter 16/

➥CN=shadrach.ispnet1.net

i:/C=US/ST=Indiana/L=Indianapolis/O=E-mail book/OU=Chapter 16/

➥CN=shadrach.ispnet1.net

--

Server certificate

--BEGIN CERTIFICATE-----

MIIDPzCCAqigAwIBAgIBADANBgkqhkiG9w0BAQQFADB5MQswCQYDVQQGEwJVUzEQ

MA4GA1UECBMHSW5kaWFuYTEVMBMGA1UEBxMMSW5kaWFuYXBvbGlzMRYwFAYDVQQK

--END CERTIFICATE-----

subject=/C=US/ST=Indiana/L=Indianapolis/O=E-mail book/OU=Chapter 16/

➥CN=shadrach.ispnet1.net

issuer=/C=US/ST=Indiana/L=Indianapolis/O=E-mail book/OU=Chapter 16/

➥CN=shadrach.ispnet1.net

--

No client certificate CA names sent

--

SSL handshake has read 989 bytes and written 320 bytes

--

New, TLSv1/SSLv3, Cipher is DES-CBC3-SHA

Server public key is 1024 bit

SSL-Session:

Protocol : TLSv1

Cipher : DES-CBC3-SHA

Session-ID:
8AC70E01DDBF80E5027D110C490D3BDAAE8031312AC8CC01904A58471AE

Session-ID-ctx:

Master-Key:
F276BD43CE6293E1E93390E9426F0940B83C1A0F0E8488C3C7B72BCB604

Key-Arg : None

Start Time: 995731589

Timeout : 300 (sec)

Verify return code: 18 (self signed certificate)

--

+OK POP3 localhost v2001.76 server ready

USER rich

+OK User name accepted, password please

PASS guitar

+OK Mailbox open, 0 messages

LIST

+OK Mailbox scan listing follows

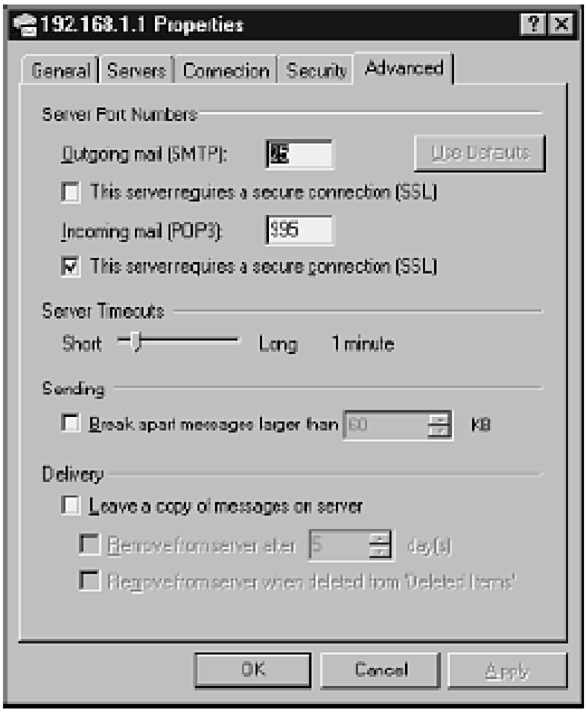
.

QUIT

DONE

همچنین این بسته، از پورت ۹۹۳ برای IMAP به همراه ssl استفاده می‌کند.

برای پیکربندی کلاینت نیز، بایستی بر روی کلاینت، تنظیماتی انجام داد[2]. شکل ٤-۱۲ تنظیمات مورد نیاز را، بر روی Microsoft Outlook نشان می‌دهد.



شکل (٤-۱۲) : فعال کردن ssl بر روی Microsoft outlook

محاسبه میزان کاهش مخاطره

در آزمایش صورت گرفته برای امن کردن پروتکل‌های pop3 و imap، از ssl استفاده شد. از نرم افزار openssl، برای تولید گواهی‌ها بهره برده ایم. از ۱۰۰ پیام فرستاده شده، امکان انجام هیچ گونه سوء استفاده‌ای، وجود نداشت. برای انجام این تست، از نرم افزار ethereal استفاده شد تا پیام‌ها را capture کنیم. همچنین هیچ ابزاری برای نفوذ و در هم شکستن SSL یافت نشد.

جدول (٤-١٩) : میزان کاهش مخاطره نا امن بودن پروتکل‌های Imap, pop3

نام مخاطره	مخاطره ناامن پروتکل‌های imap و pop3
شناسایی و محافظت	استفاده از SSL و TLS
تعداد آزمایش‌های صورت گرفته	۱۰۰- ابزاری برای نفوذ و در هم شکستن SSL یافت نشد.
تعداد حملات موفق	۰
حملات نا موفق	۱۰۰ - ابزاری برای نفوذ و در هم شکستن SSL یافت نشد.
جمع امتیاز قبل از ایمن سازی	۲۹
میزان کاهش مخاطره(درصد)	۱۰۰
جمع امتیاز پس از ایمن سازی	۰

۴-۲-۶ امن کردن سرورهای Webmail

اگر بخواهید webmail، بر روی محیط امنی اجرا شود به بسته‌های openssl و apache mod_ssl نیاز دارید تا اتصال SSL HTTP امنی را برقرار کنید[2].

امن کردن سرور MySql

اکثر بسته‌های متن باز webmail رایجی که وجود دارند، دارای پایگاه داده MySql می‌باشند. برای امن کردن webmail، گام اول این است که MySql را امن کنید. کارهای زیر را برای امن کردن MySql، می‌توان توصیه نمود[58]:

- تعویض گذرواژه پیش فرض root، برای Mysql باعث می‌شود کار نفوذ گر سخت‌تر شود.

- تغییر مجوزهای پوشه‌های پایگاه داده که با مالک کردن کاربر با نام mysql، انجـام می‌گیرد، باعث می‌شود که نفوذ گر نتواند بـا مجـوز root، سیسـتم را مـورد سـوء استفاده قرار دهد.

امن کردن سرور Apache

مهم‌ترین بخش امن کردن سرور webmail، امن کردن سرور وب می‌باشد. Apache محبوب‌ترین و رایج‌ترین بسته متن باز سرور وب می‌باشد. یکی از ماژول‌های موجود برای apache، mod_ssl می‌باشد که برای افزودن پروتکل ssl، به نرم افزار سرور وب استاندارد، بکار می‌رود و باعث ایجاد متدی امن، برای انتقال داده بین کلاینت و سرور وب می‌شود[59].

برای استفاده و نصب mod_ssl، بایستی برنامه openssl نصب شده باشد. برای استفاده از ویژگی سرور وب ssl، بایستی یک گواهی دیجیتالی معتبر، داشته باشید. می‌توانید این گواهی را از یک فروشنده تجاری بخرید یا اینکه خودتان گواهی را توسط apache ایجاد کنید. اگر به کاربران خارج از سازمان، سرویس می‌دهید بایستی گواهی را از فروشنده تجاری بخرید تا کاربران بتوانند، اعتماد کنند و ارزیابی کنند که سرور وب، تایید هویت شده است. اگر گواهی را خریده باشید، بایستی مکان آن را به apache بگویید. دستور زیر این مسئله را نشان می‌دهد.

./configure —with-apache=/usr/local/src/apache_1.3.20 with-
crt=*/path/to/server.crt* —with-key=*/path/to/server.key*

همچنین مکان برنامه openssl را نیز بایستی به apache بگویید.

$ **SSL_BASE=/usr/local/ssl **

اگر گواهی را از یک شرکت تجاری نخرید، بایستی خودتان آن را ایجاد کنید. این کار را با دستور make certificate انجام می‌دهید.

برای استفاده از ssl در apache، پورت ٤٤٣ بایستی به صورت زیر پیکربندی شود.

<VirtualHost _default_:443>

در نهایت، بایستی برنامه webmail را برای استفاده از ویژگی‌هـای ارائـه شـده، پیکـر بنـدی کنید.

محاسبه میزان کاهش مخاطره

در آزمایش صورت گرفته موارد زیر، انجام گرفت:

- برای تأمین امنیت سرور وب، از SSL استفاده شد و گواهی را خودمان تولید نمودیم.
- نکته‌هایی که برای تأمین امنیت mySql ذکر شد، انجام گرفت.
- توسط سیستم عامل Windows Xp SP3 که بر روی Vmware نصب بود، تست‌ها صورت گرفت.
- از مرور گر IE7، برای تست استفاده کردیم.
- از webmail ی بنام squirrel mail استفاده نمودیم[60].
- SSL بر روی سرور پست الکترونیکی فعال شد.
- در آزمایش صورت گرفته، ابزاری برای نفوذ و در هم شکستن SSL یافت نشد.

جدول (٤-٢٠) : میزان کاهش مخاطره نا امن بودن webmail

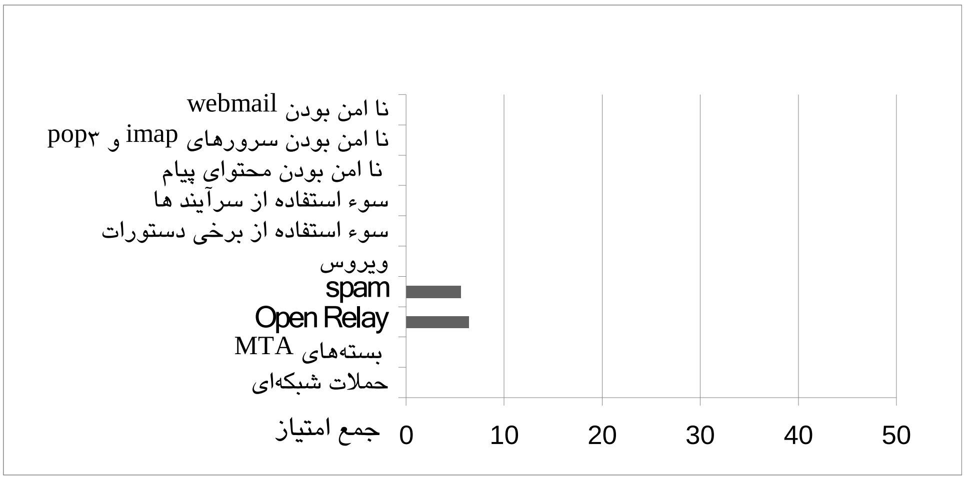
نام مخاطره	مخاطره ناامن بودن محتوی پیام
شناسایی و محافظت	استفاده از s-mime
تعداد آزمایش‌های صورت گرفته	ابزاری برای نفوذ و در هم شکستن SSL یافت نشد.
تعداد حملات موفق	۰
حملات نا موفق	ابزاری برای نفوذ و در هم شکستن SSL یافت نشد.
جمع امتیاز قبل از ایمن سازی	٤٢
میزان کاهش مخاطره(درصد)	۱۰۰
جمع امتیاز پس از ایمن سازی	۰

۴-۳ جدول و نمودار کلی

پس از ارائه جدول جزئی برای هر کاهش مخاطره که به صورت مطالعه موردی بود، جدول کلی بر حسب درصد، برای کاهش مخاطرات ارائه می‌دهیم. در نهایت، نمودار جمع امتیاز پس از کاهش مخاطره را به صورت گرافیکی ترسیم می‌کنیم.

جدول (٤-٢١) : جدول کلی کاهش مخاطرات

نام مخاطره	جمع امتیاز	درصد کاهش مخاطره	جمع امتیاز پس از کاهش مخاطره
حملات شبکه ای و دسترسی شبکه ای	٣٥	١٠٠	٠
مخاطرات بسته‌های MTA	٣٢	١٠٠	٠
مخاطره Open Relay	٣٢	٨٠	٦.٤
مخاطره spam	٤٣	٨٧	٥.٥٩
مخاطره ویروس	٤٧	١٠٠	٠
سوء استفاده از برخی دستورات و کاوش گری	٢٣	١٠٠	٠
سوء استفاده از سرآیندهای پست الکترونیکی	٣٠	١٠٠	٠
مخاطره نا امن بودن محتوای پیام	٢٦	١٠٠	٠
مخاطره نا امن بودن سرورهای imap و pop3	٢٩	١٠٠	٠
مخاطره نا امن بودن webmail	٤٢	١٠٠	٠
جمع	٣٣٩		



شکل (٤-۱۳) : نمودار کلی کاهش مخاطرات

فصل پنجم

نتیجه‌گیری و پیشنهادات

۵-۱ نتیجه گیری

در جمع بندی از نتایج این کتاب باید گفت، کمکی که این کتاب به دنیای امنیت پست الکترونیکی می‌کند این است که علاوه بر اینکه به بررسی مخاطرات پست الکترونیکی و ایمن سازی آنها می‌پردازد، روشی خاص برای ارزیابی مخاطرات پست الکترونیکی، ارائه داده است که قبل از این، برای حوزه پست الکترونیکی ارائه نشده بود. با استفاده از این روش ارزیابی مخاطره پست الکترونیکی، می‌توان روش ایمن سازی مخاطرات پست الکترونیکی با توجه به نوع سازمان، ارائه داد.

تمامی فرضیه‌های موجود برای این کتاب که در فصل اول معرفی کردیم، تایید شدند:

- سیستم پست الکترونیکی، دارای مکانیزم‌ها و پروتکل‌های مختلفی می‌باشد. این مکانیزم‌ها و پروتکل‌ها، حاوی مخاطراتی می‌باشند و می‌توان این مخاطرات را شناسایی کرد.
- می‌توان مخاطرات موجود در سیستم‌های پست الکترونیکی را ارزیابی کرد.
- می‌توان از روش‌های ارزیابی مخاطراتی که در سایر سیستم‌ها وجود دارد، برای سیستم پست الکترونیکی نیز استفاده نمود.
- پارامترهای موجود در ارزیابی مخاطرات سایر سیستم‌ها، با مکانیزم‌ها و پروتکل‌های سیستم پست الکترونیکی، نیز رابطه دارند.
- می‌توان مخاطرات موجود در پست الکترونیکی را با روش‌های موجود ایمن نمود.
- می‌توان میزان کاهش مخاطره را پس از ایمن سازی، محاسبه کرد.
- می‌توان راهکاری جامع، بر اساس تقسیم بندی سازمان‌ها و میزان مخاطره ارائه داد.

این کتاب، در واقع نگاهی جامع به مقوله امنیت سرور و سرویس پست الکترونیکی داشت. در ابتدا، مخاطرات سرور و سرویس پست الکترونیکی، بررسی گردید و با جداول و فرمولی که ارائه شد، مخاطرات را امتیاز بندی نمودیم. پس از آن به راهکارهای ایمن سازی سرویس و سیستم پست الکترونیکی پرداختیم. آزمایش‌هایی برای بررسی کاهش مخاطره، انجام شدند که در واقع، هر آزمایش، به صورت مطالعه موردی بود و امتیاز کلی پس از کاهش مخاطره محاسبه شد. فعالیت‌های صورت گرفته، در دو دسته کلی ایمن سازی سرور و سرویس پست الکترونیکی بررسی شدند.

در قسمت مخاطرات سرور پست الکترونیکی و راهکارهای ایمن سازی، به موارد زیر پرداختیم:

- فعال نبودن برخی ویژگی‌ها بر روی سرور پست الکترونیکی، می‌تواند باعث به مخاطره افتادن سرور و سوء استفاده از آن گردد. این ویژگی‌ها را بررسی کرده و نحوه فعال کردن آنها را بیان کردیم.
- مخاطره open realy بر روی سرور پست الکترونیکی، بررسی گردید. مکانیزم‌های رله کردن گزینشی برای جلوگیری از open relay شدن، ارائه شد.
- مخاطره spam معرفی و ۳ متد کلی برای بلوک کردن spam ارائه شد.
- مخاطره ویروس‌ها بررسی شد و مکانیزم ایمن سازی ارائه شد.

در قسمت مخاطرات سرویس پست الکترونیکی و راهکارهای ایمن سازی، به موارد زیر پرداختیم:

- نفوذکنندگان و spammerها، تکنیک‌های مختلفی استفاده می‌کنند تا اطلاعاتی در مورد سیستم پست الکترونیکی و کاربران آن بدست آورند، تکنیک‌هایی ارائه دادیم که کمک می‌کنند تا با این مشکل، مبارزه کنید. با غیر فعال کردن برخی دستورات و همچنین نصب فایروال پست الکترونیکی، می‌توانید جلوی حملات و کاوشگری‌ها را بگیرید.
- متد رایج اجازه دادن به میزبان‌های راه دور که بتوانند پیام‌ها را از طریق پست الکترونیکی سرور، رله کنند، استفاده از یک متد تایید هویت می‌باشد. متد تایید هویت به صورت منحصربه‌فرد، می‌تواند پست الکترونیکی سرور راه دور را مشخص کند به نحوی که پست الکترونیکی سرورتان، بتواند مشخص کند اجازه

دارد پیام‌ها را رله کند یا خیر. یکی از مشهورترین متدهای تایید هویت اتصالات شبکه SASL[1] می‌باشد که آن را بررسی کردیم.

- بسیاری از بسته‌های MTA[2]، برای دریافت پیام‌ها از پروتکل‌های pop3[3] یا imap[4] بهره می‌گیرند. مشکل این پروتکل‌ها این است که آنها اطلاعات را به صورت متن اسکی، بدون هیچ رمز نگاری ارسال می‌کنند. برای کمک کردن به این‌گونه مسائل پروتکل SSL[5] به وجود آمد که به میزبان‌های شبکه اجازه می‌دهد تا داده‌ها را قبل از ارسالشان در طول شبکه، رمز کنند. که به شرح این پروتکل و پروتکل‌های مشابه آن پرداختیم.
- بسیاری از شرکت‌ها، نرم افزار کلاینتی پست الکترونیکی تحت وب، منتشر کرده‌اند که کاربر را قادر می‌سازد از طریق وب، پست الکترونیکی خود را بخواند. پیاده سازی‌های بسیار زیاد و محبوبی مانند Hotmail، Yahoo! و Gmail وجود دارد که کاربران می‌توانند از طریق پویش گر وب[6]، به سرور پست الکترونیکی متصل شوند. Webmail به خودی خود، امن نیست و به راهکارهای ایمن سازی آن اشاره شد.

در نتیجه گیری کلی، سه راهکار ایمن سازی، برای سه گونه پست الکترونیکی، ارائه می‌دهیم:

- پست الکترونیکی‌های با امنیت متوسط

- پست الکترونیکی‌های با امنیت بالا

- پست الکترونیکی‌های با امنیت بالا به همراه محرمانگی

در تقسیم بندی انجام گرفته توسط سازمان فناوری اطلاعات ایران، سازمان‌ها به ٤ دسته اجرایی، ملی، حساس و اجرایی حیاتی تقسیم بندی شده‌اند[61]. با استفاده از این تقسیم بندی، سازمان‌ها را از لحاظ نیاز پست الکترونیکی، در گروه‌های زیر قرار می‌دهیم:

- پست الکترونیکی‌های با امنیت متوسط، برای سازمان‌های اجرایی.
- پست الکترونیکی‌های با امنیت بالا، برای سازمان‌های ملی.

---

1 Simple Authentication and Security Layer
2 Mail Transfer Agent
3 Post Office Protocol version 3
4 Internet Message Access Protocol
5 Secured Socket Layer
6 Web Browser

- پست الکترونیکی‌های با امنیت بالا به همراه محرمانگی، برای سازمان‌های حساس و اجرایی حیاتی.

۵-۱-۱ پست الکترونیکی‌های با امنیت متوسط برای سازمان‌های اجرایی

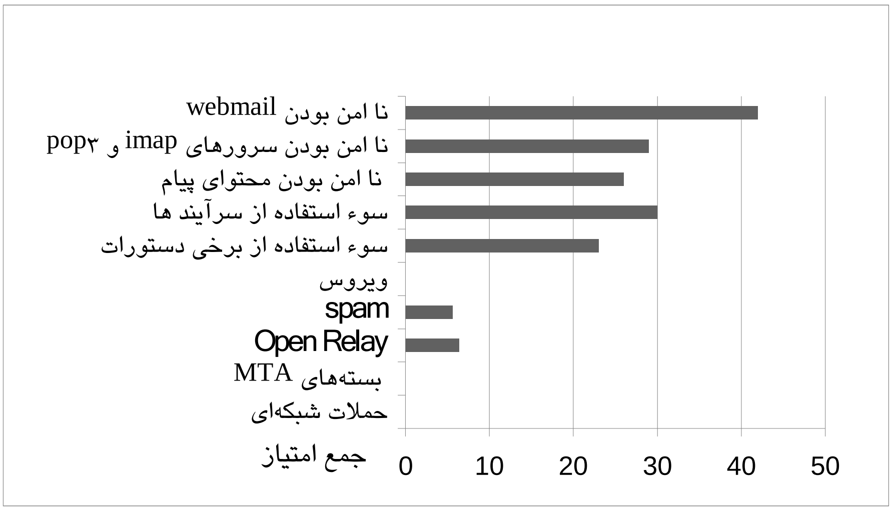
در این گونه پست الکترونیکی، امنیت چندان اهمیت ندارد و صرف اینکه بتوان پیامی ارسال و دریافت کرد برای فرد استفاده کننده، کافیست. سازمان‌های اجرایی و محیطهایی که امنیت پست الکترونیکی در آنها چندان اهمیت ندارد، از این گونه می‌باشند.

در اینجا مسئله مهم، تأمین امنیت سرور پست الکترونیکی می‌باشد نه تأمین سرویس پست الکترونیکی. علت این است که می‌خواهیم سرور، پابرجا باشد و کار خود را ادامه دهد، حال اینکه محتوای پیام، ایمن بماند یا اینکه کسی از پروتکل‌های imap یا pop3 سوء استفاده کند و بتواند پیام دیگران را بخواند، چندان مهم نیست. ولی اگر ویروسی به سرور اثر کند، کل سرور از هم می‌پاشد یا اینکه حجم پست الکترونیکی‌های spam یاopen relay، به حدی شود که حمله DOS صورت بگیرد، سرور از کار می‌افتد. به این دلیل توصیه می‌شود مخاطرات زیر ایمن شوند:

- مخاطرات حمله شبکه ای و دسترسی شبکه ای
- مخاطره بسته‌های MTA
- مخاطره Open Relay
- مخاطره Spam
- مخاطره ویروس

جدول (۵-۱) : راهکار پست الکترونیکی با امنیت متوسط برای سازمان‌های اجرایی

نام مخاطره	ایمن سازی مخاطره	جمع امتیاز
حملات شبکه ای و دسترسی شبکه ای	بلی	۰
مخاطرات بسته‌های MTA	بلی	۰
مخاطره Open Relay	بلی	٦.٤
مخاطره spam	بلی	٥.٥٩
مخاطره ویروس	بلی	۰
سوء استفاده از برخی دستورات و کاوش گری	خیر	۲۳
سوء استفاده از سرآیندهای پست الکترونیکی	خیر	۳۰
مخاطره نا امن بودن محتوای پیام	خیر	۲٦
مخاطره نا امن بودن سرورهای imap و pop3	خیر	۲۹
مخاطره نا امن بودن webmail	خیر	٤۲
جمع		١٦١.٩٩



شکل (۵-۱) : نمودار راهکار پست الکترونیکی با امنیت متوسط برای سازمان‌های اجرایی

۵-۱-۲ پست الکترونیکی‌های با امنیت بالا برای سازمان‌های ملی

در این گونه پست الکترونیکی، امنیت اهمیت دارد و صرف اینکه بتوان پیامی ارسال و دریافت کرد، برای فرد استفاده کننده کافی نیست. سازمان‌های ملی جزء این دسته هستند.

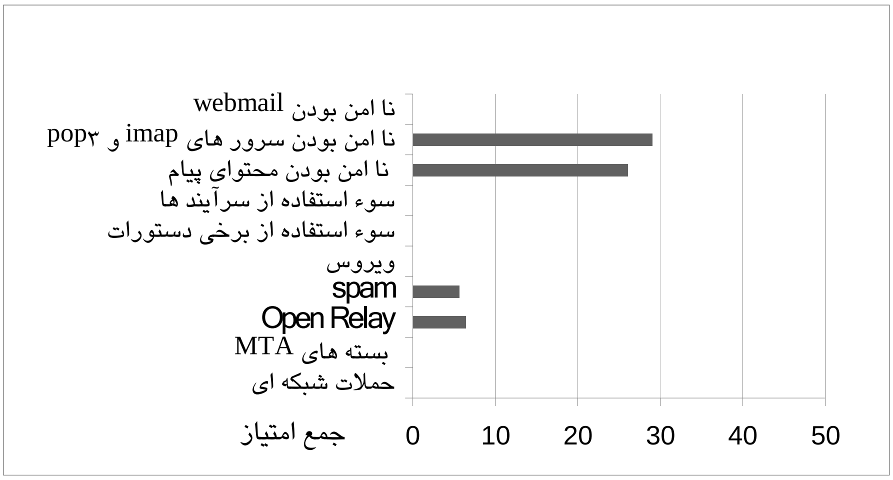
در اینجا مسئله مهم، هم تأمین امنیت سرور پست الکترونیکی می‌باشد هم تأمین سرویس پست الکترونیکی. چون در اینجا علاوه بر اینکه می‌خواهیم، سرور پابرجا باشد و کار خود را ادامه دهد، بایستی از سرویس پست الکترونیکی، سوءاستفاده نشود. اما در اینجا محرمانه بودن پیام، برای همه ضروری نیست. به این دلایل، توصیه می‌شود مخاطرات زیر ایمن شوند:

- مخاطرات حمله شبکه ای و دسترسی شبکه ای
- مخاطره بسته‌های MTA
- مخاطره Open Relay
- مخاطره Spam
- مخاطره ویروس

- مخاطره سوء استفاده از برخی دستورات و کاوش گری
- مخاطره سوء استفاده از سرآیندهای پست الکترونیکی
- مخاطره نا امن بودن webmail

جدول (۵-۲) : راهکار پست الکترونیکی با امنیت بالا برای سازمان‌های ملی

نام مخاطره	ایمن سازی مخاطره	جمع امتیاز
حملات شبکه ای و دسترسی شبکه ای	بلی	۰
مخاطرات بسته‌های MTA	بلی	۰
مخاطره Open Relay	بلی	٦.٤
مخاطره spam	بلی	٥.٥۹
مخاطره ویروس	بلی	۰
سوء استفاده از برخی دستورات و کاوش گری	بلی	۰
سوء استفاده از سرآیندهای پست الکترونیکی	بلی	۰
مخاطره نا امن بودن محتوای پیام	خیر	٢٦
مخاطره نا امن بودن سرورهای imap و pop3	خیر	٢۹
مخاطره نا امن بودن webmail	بلی	۰
جمع		٦٦.۹۹



شکل (۵-۲) : نمودار راهکار پست الکترونیکی با امنیت بالا برای سازمان‌های ملی

۵-۱-۳ پست الکترونیکی‌های با امنیت بالا به همراه محرمانگی، برای سازمان‌های حساس و اجرایی حیاتی

در این گونه پست الکترونیکی، امنیت اهمیت بسیار بالایی دارد و صرف ایمن بودن سرور و سرویس پست الکترونیکی، کافی نیست. پست الکترونیکی سازمان‌های امنیتی و نظامی و نامه‌های محرمانه ادارات دولتی، از این گونه پست الکترونیکی می‌باشند. سازمان‌های حساس و اجرایی حیاتی، جزء این دسته می‌باشند.

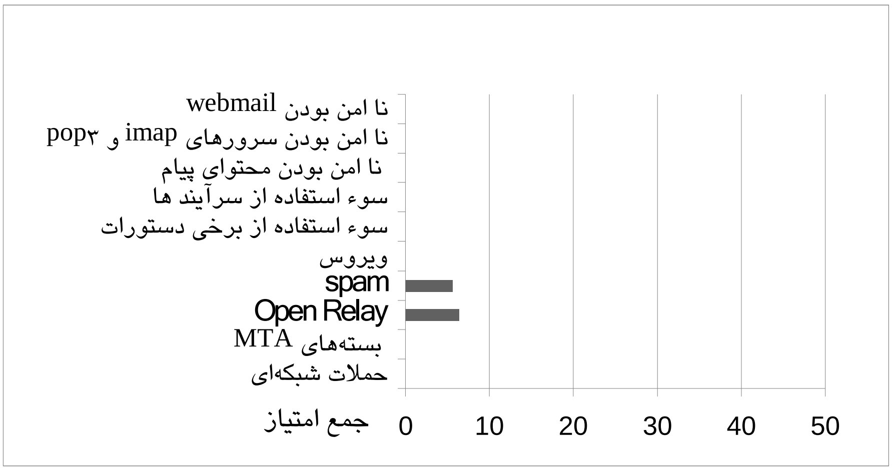
در اینجا مسئله مهم، علاوه بر تأمین امنیت سرور و سرویس پست الکترونیکی، محرمانه ماندن پیام می‌باشد. به این دلایل توصیه می‌شود مخاطرات زیر ایمن شوند:

- مخاطرات حمله شبکه ای و دسترسی شبکه ای
- مخاطره بسته‌های MTA
- مخاطره Open Relay
- مخاطره Spam
- مخاطره ویروس
- مخاطره سوء استفاده از برخی دستورات و کاوش گری

- مخاطره سوء استفاده از سرآیندهای پست الکترونیکی
- مخاطره نا امن بودن webmail
- مخاطره نا امن بودن سرورهای imap و pop3
- مخاطره نا امن بودن محتوای پیام

جدول (۵-۳) : راهکار پست الکترونیکی با امنیت بالا به همراه محرمانگی برای سازمان‌های حساس و اجرایی حیاتی

نام مخاطره	ایمن سازی مخاطره	جمع امتیاز
حملات شبکه ای و دسترسی شبکه ای	بلی	۰
مخاطرات بسته‌های MTA	بلی	۰
مخاطره Open Relay	بلی	٦.٤
مخاطره spam	بلی	۵.۵۹
مخاطره ویروس	بلی	۰
سوء استفاده از برخی دستورات و کاوش گری	بلی	۰
سوء استفاده از سرآیندهای پست الکترونیکی	بلی	۰
مخاطره نا امن بودن محتوای پیام	بلی	۰
مخاطره نا امن بودن سرورهای imap و pop3	بلی	۰
مخاطره نا امن بودن webmail	بلی	۰
جمع		۱۱.۹۹



شکل (۵-۳) : نمودار راهکار پست الکترونیکی با امنیت بالا به همراه محرمانگی برای سازمان‌های حساس و اجرایی حیاتی

فصل ششم

مراجع و منابع

[1] Ferris, M. ,"New Email Security Infrastructure ", IEEE Conferences , 1994 , Page(s): 20 – 27

[2] RICHARD BLUM , "Open Source E-mail Security" , Sams, 2002

[3] Peter Piazza,"Closing open relays to spammers",Tech Talk, Jul 31, 2005

[4] Shirali-Shahreza, S.; Movaghar, A."A New Anti-Spam Protocol Using CAPTCHA", IEEE Conferences , 2007 , Page(s): 234 - 238

[5] Faure, F.; Lopusniac, M.; Richard, G.; Farmer, M.; "A complexity-based method for anti-spamming", IEEE Conferences , 2007 , Page(s): 315 – 320

[6] James Stanger ,"E-mail Virus Protection Handbook : Protect your E-mail from Viruses, Tojan Horses, and Mobile Code Attacks" Syngress,Oct 30, 2000

[7] K. Zeilenga," Anonymous Simple Authentication and Security Layer (SASL) Mechanism ", RFC 4505, June 2006

[8] A. Melnikov, Ed., K. Zeilenga, Ed.," Simple Authentication and Security Layer (SASL)" , RFC4422, June 2006

[9] Myers, J. , Rose, M. , " Post Office Protocol - Version 3", RFC 1939, May 1996

[10] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL – VERSION 4rev1", RFC 3501, March 2003.

[11] Rolf Oppliger ,"SSL and TLS: Theory and Practice (Information Security and Privacy)" , Artech House,Sep 30, 2009

[12] Curtis Smith,"Pro Open Source Mail: Building an Enterprise Mail Solution",apress Sep 26, 2006

[13] Gary Stoneburner, Alice Goguen, and Alexis Feringa," Risk Management Guide for Information Technology Systems", *Recommendations of the National Institute of Standards and Technology* , NIST Special Publication 800-30, July 2002

[14] G. McGraw, “Software Security,”*IEEE Security & Privacy*, vol. 2, no.2, 2004, pp. 80–83.

[15] Sushila Madan; Supriya Madan ,"Bulwark Against SQL Injection Attack– An Unified Approach",IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010

[16] Cisco Systems Learning,"Implementing Cisco Intrusion Prevention Systems Volume 1 Version 6.0", Cisco Press, 2006

[17] Sean Convery, "Network Security Architectures" , Cisco Press ,2004

[18] Jain, Y.K.; Gosavi, P.B , " Email Security Using Encrption and Compression" , IEEE Conferences , 2008 , Page(s): 136 – 139

[19] Stephen Farrell , " Why Don't We Encrypt Our Email " , IEEE JOURNALS , 2009 , Page(s): 82 – 85

[20] Zou, C.C.; Towsley, D.; Weibo Gong;" Email Worm Modeling and defense ", IEEE CONFERENCES , 2004 , Page(s): 409 – 414

[21] D'Ambra, D , " Killer spam: clawing at your door " , IET JOURNALS , 2007, Page(s): 28 – 3

[22] D'Ambra, D , " Spam spotting man v computer " , IET JOURNALS , 2008 , Page(s): 58 – 60

[23] Crocker ,D , "Internet Mail Architecture " , IETF RFC 5598, July 2009

[24] Klensin, J., "Simple Mail Transfer Protocol",RFC 5321, October 2008

[25] Klensin, J., Freed, N., Rose, M., Stefferud, E., and D. Crocker, "SMTP Service Extensions", STD 10, RFC 1869, November 1995.

[26] J. Postel, "Simple Mail Transfer Protocol", RFC 821, August 1982

[27] C. Malamud ,"A No Soliciting Simple Mail Transfer Protocol (SMTP) Service Extension" ,RFC 3865, September 2004

[28] E. Allman, T. Hansen,"SMTP Service Extension for Message Tracking", RFC 3885, September 2004

[29] E. Allman, H. Katz,"SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail Message", RFC 4405, April 2006

[30] Freed, N., Borenstein, N., "Multipurpose Internet Mail Extensions (MIME)",RFC 2045, November 1996

[31] Sample Size Calculator ,[Online].<http://www.surveysystem.com/sscalc.htm> , [18 December 2010]

[32] Daniel J. Barrett, Richard E. Silverman, and Robert G. Byrnes ,"Linux Security Cookbook" ,O'Reilly ,Jun 2003

[33] Bryan Costales, Claus Assmann, George Jansen, and Gregory Neil Shapiro ,"sendmail, 4th Edition" , O'Reilly,Oct 26, 2007

[34] John R. Levine ,qmail,O'Reilly, Feb 2004

[35] Dave Sill ,"The qmail Handbook",Apress, Oct 2001

[36] Patrick Ben Koetter,"Postfix",dpunat.veriag ,2008

[37] Kyle D. Dent, "Postfix: The Definitive Guide", O'Reilly, Dec 2003

[38] Hambridge, S., Lunde, A., "DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)", RFC 2635, June 1999

[39] Schwartz, Alan and Simson Garfinkel, "Stopping Spam" , O'Reilly and Associates, 1998

[40] Jungsuk Song; Inque, D.; Eto, M.; Hyung Chan Kim; Nakao, K.,"An Empirical Study of Spam: Analyzing Spam Sending Systems and Malicious Web Servers", IEEE Conferences , 2010 , Page(s): 257 - 260

, RFC 2076, February 1997"

[41] Palme, J. ,"Common Internet Message Headers

[42] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka, " S/MIME Version 2 Message Specification ", RFC 2311, March 1998

[43] M. Elkins, D. Del Torto, R. Levien, T. Roessler, "MIME Security with OpenPGP ", RFC 3156, August 2001

[44] T. Dierks, E. Rescorla," The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006

[45] Lux, K.D.; May, M.J.; Bhattad, N.L.; Gunter, C.A.,"WSEmail: secure Internet messaging based on Web services", IEEE Conferences, 2005 , Page(s): 75 - 82 vol.1

[46] Evi Nemeth, Garth Snyder, Trent R. Hein, and Ben Whaley ,"UNIX and Linux System Administration Handbook (4th Edition)" Jul 2010

[47] Gregor N. Purdy ,"Linux iptables Pocket Reference",O'Reilly,Nov 2004

[48] Murali, A.; Rao, M ,"A Survey on Intrusion Detection Approaches" , IEEE Conferences ,2005 , Page(s): 233 - 240

[49] Craig Hunt ,"Linux Sendmail Administration (Craig Hunt Linux Library)",Sybex ,Mar 2001

[50] Martin McCarthy ,"The Procmail Companion (Practical Solutions Series)", Netrorking Solutions, Nov 2001

[51] Brian Hatch, James B. Lee, and George Kurtz ,"Linux (Hacking Exposed)" ,O'Reilly,Mar 2001

[52] Liu, W.W.,"Identifying and Addressing Rogue Servers in Countering Internet Email Misuse", IEEE Conferences , 2010 , Page(s): 13 - 24

[53] Dhinakaran, C.; Jae Kwang Lee; Nagamalai, D., "An Empirical Study of spam and spam Vulnerable email Accounts", IEEE Conferences , 2007 , Page(s): 408 - 413

[54] Alistair McDonald,"SpamAssassin: A Practical Guide to Integration and Configuration",packt,2004

[55] A Mail Virus Scanner ,[Online].<http://www.amavis.org> , [21 December 2010]

[56] James Turnbull,Hardening Linux , Apress, Feb 2005

[57] R. Siemborski, Ed., A. Melnikov, Ed. , "SMTP Service Extension for Authentication ", RFC 4954, July 2007

[58] Wrox Author Team,"Mysql Security Handbook",Wrox,Sep 2003

[59] Ivan Ristic, "Apache Security",O'Reilly,Mar 2005

[60] SquirrelMail,[Online].< http://squirrelmail.org/> , [21 December 2010]

[61] سازمان فناوری اطلاعات ایران ,[Online].< http://www.itc.ir> , [22 December 2010]